

# CTRL + ALT + PROTECT

## सुरक्षा नगर की रोमांचक यात्रा

### इंटरनेट पर सुरक्षित रहने की आसान गाइड



# विषयसूची

यह हैंडबुक इंटरनेट को मजेदार तरीके से और सुरक्षित रूप से एक्सप्लोर करने में मदद करेगी। सात दोस्तों की कहानियों के ज़रिए आप जानेंगे स्कैम्स, प्राइवैसी, मिसइन्फॉर्मेशन और इंटरनेट जिम्मेदारी के बारे में

क्र.	शीर्षक	विवरण	पृष्ठ संख्या
	पात्र और परिचय	चलिए मिलते हैं सुरक्षा नगर के दोस्तों की टोली से।	1-3
चैप्टर 1	हैलो डिजिटल दुनिया!	अपने ऑनलाइन आदतों, डिजिटल फुटप्रिंट के बारे में सोचेंगे और एक बेहतर डिजिटल दुनिया की अपनी कल्पना पर विचार करेंगे।	4-16
चैप्टर 2	स्कैम्स, हैक्स और साइबर हमले: होशियार रहो!	यहाँ बात करेंगे हैकिंग, फ़िशिंग, पहचान चोरी और ऑनलाइन शॉपिंग के स्कैम्स के बारे में। साथ ही सीखेंगे पासवर्ड्स और टू-फ़ैक्टर ऑथेंटिकेशन जैसे डिजिटल सुरक्षा टूल्स के बारे में।	17-37
चैप्टर 3	गोपनीयता: आपकी डिजिटल ढाल	प्राइवैसी सेटिंग्स, ऑनलाइन बातचीत और गेमिंग में कैसे अपनी सीमाएँ तय करें ताकि साइबर स्टॉकिंग, डॉक्सिंग जैसी चीज़ों से बच सकें।	38-56
चैप्टर 4	सोचें, समझें, फिर क्लिक करें: मिसइन्फॉर्मेशन से बचने के टिप्स	फेक न्यूज़, बायस और क्लिकबेट को पहचानें! AI से बनी तस्वीरें, वीडियो, एल्गोरिदम और ऑनलाइन उपलब्ध जानकारी के प्रभाव के बारे में भी जानें।	57-84
चैप्टर 5	गेम ओवर स्कैमर्स - ऑनलाइन खतरों को पहचाने और रोके!	स्कैम और खतरों को पहचानें, सही समय पर रिपोर्ट करें और ज़रूरत पड़ने पर मदद लें। साथ में कानूनों के बारे में भी जानें।	85-101
चैप्टर 6	क्लिक, स्क्रोल, आराम! डिजिटल दुनिया में सुकून	चलो सीखें की इंटरनेट इंटरनेट का इस्तेमाल समझदारी और सुरक्षित तरीके से कैसे किया जाए। ऑनलाइन परेशानी में इमोशनल और सोशल सहायता कैसे करते हैं?	102-109
चैप्टर 7	ऑनलाइन आवाज़ उठाओ, बदलाव लाओ!	इंटरनेट का इस्तेमाल कर के हम कैसे एक-दूसरे की मदद कर सकते हैं, कैसे आवाज़ उठा सकते हैं, और एक सेफ ऑनलाइन कम्युनिटी बना सकते हैं।	110-121

सुरक्षा नगर नामक एक खुशनुमा शहर में सात अच्छे दोस्त रहते थे - मीरा, रहीम, जसप्रीत, सुजैन, शुभम, सिद्धार्थ और नूर।



सुरक्षा नगर में दोपहर का समय था और मीरा के घर का आरामदायक लिविंग रूम शोर और हंसी से भरा हुआ था। सातों दोस्त- मीरा, रहीम, परवीन, सुज़ैन, शुभम, सिद्धार्थ और नूर- सोफे और फर्श पर बैठे हुए थे, उनके चारों ओर स्नेक्स बिखरे हुए थे, और वे एक पुराने लैपटॉप को चालू कर रहे थे।

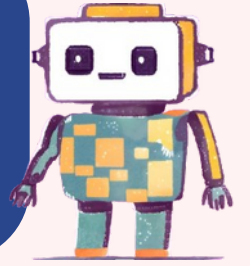
"चलो इसे देखते हैं!" मीरा ने उत्सुकता से कहा, उसकी उंगलियाँ पहले से ही अलग-अलग साइटों और खेलों पर क्लिक कर रही थीं। "रुको, जल्दी मत करो! तुम गलती से किसी अजीब चीज़ पर क्लिक कर सकती हो," रहीम ने एक भौंह सिकोड़ कर आगे झुकते हुए चेतावनी दी। "रहीम, इतनी चिंता मत करो - सब ठीक है," शुभम ने चिढ़ाते हुए कहा, उसने ग्रुप को अपने नोटिफिकेशन से गूँजते फ़ोन में एक मज़ेदार मीम दिखाया।

"क्या तुमने जाँचा कि यह साइट सुरक्षित है?" जसप्रीत ने पूछा, उनकी जासूसी प्रवृत्तियाँ स्क्रीन पर नज़र डालते ही सक्रिय हो गईं। "और कुछ भी व्यक्तिगत शेयर मत करना," सुज़ैन ने कहा, उसका स्वर शांत लेकिन दृढ़ था, और साथ ही वह पहले से बुकमार्क की गई नई गोपनीयता गाइड को स्करोल कर रही थी। सिद्धार्थ ने ठहाका लगाया और कहा, "ठीक है, सब लोग साँस लो! हम बस चीज़ें सर्च कर रहे हैं - घबराने की कोई ज़रूरत नहीं है," उसकी सहज आवाज़ ने सभी को शांत रहने में मदद की। इस बीच, नूर अपनी नोटबुक में विचार लिख रही थी। "क्या होगा अगर हम इंटरनेट का उपयोग करने के सबसे अच्छे, सबसे सुरक्षित तरीकों के बारे में एक प्रोजेक्ट शुरू करें? हम इसे स्कूल के साथ भी शेयर कर सकते हैं!" उसने सुझाव दिया, उसकी आँखें उत्साह से चमक रही थीं।

जैसे-जैसे वे गेम्स, वीडियोज़ और अजीब पॉप-अप्स के बीच आगे बढ़ते गए, कमरा बहस, हंसी और कभी-कभी "ओह, मेरा इरादा इसे क्लिक करने का नहीं था!" से भर गया। यह केवल इंटरनेट के बारे में नहीं था - यह एक साथ काम करने, एक-दूसरे से सीखने और यह सुनिश्चित करने के बारे में था कि उनके ऑनलाइन अनुभव सुरक्षित और मज़ेदार हों।



अमित भैया और ग्लिच के साथ, ये सभी दोस्त डिजिटल दुनिया के माध्यम से एक रोमांचक यात्रा पर निकलने वाले हैं।



वे सीखेंगे कि कैसे डिजिटल दुनिया को सुरक्षित तरीके से नेविगेट करें, छिपे हुए जोखिमों को कैसे पहचानें और इंटरनेट द्वारा प्रदान की जाने वाली अविश्वसनीय संभावनाओं को अनलॉक करें। हर क्लिक से कुछ नया पता चलेगा।

लेकिन यह सफ़र हमेशा आसान नहीं होगा। रास्ते आश्चर्यों और कुछ मुश्किलों से भरे होंगे। फिर भी, अमित भैया के मार्गदर्शन और ग्लिच की चतुर चालों से, बच्चे हर चुनौती का आत्मविश्वास के साथ सामना करेंगे। क्या वे आगे के रोमांच के लिए तैयार होंगे?



ऑनलाइन दुनिया में आगे बढ़ने के बारे में उतार-चढ़ाव और महत्वपूर्ण सबकों से भरे उनके बड़े साहसिक कारनामों में शामिल हों!

# चैप्टर 1: हैलो डिजिटल दुनिया!



मीरा अपनी माँ का फ़ोन खिड़की के पास लेकर बैठी है। फ़ोन दर्जनों खुले टैब से जगमगा रहा है। उसने हाल ही में इंटरनेट की विशाल दुनिया को एक्सप्लोर करना शुरू किया है—मजेदार वीडियो देखना, नए गाने खोजना और अपने ढेर सारे सवालों के जवाब ढूँढ़ना। उसे यह सब बहुत पसंद है, लेकिन आज वह थोड़ी उलझन में है।

मीरा ने सोचा, "इंटरनेट को हर चीज़ के बारे में इतना कुछ कैसे पता चलता है? हर चीज़ एक-दूसरे से कैसे जुड़ी हुई है?"

शुक्र है, अमित भैया पास ही थे। "भैया!" उसने आवाज दी, और थोड़ी ही देर में अमित भैया हमेशा की तरह अपनी शांत मुस्कान के साथ अंदर आ गए।

इंटरनेट इतना सब कैसे जानता है? ये सब कुछ कहाँ रखता है, और ये सब आपस में कैसे जुड़ा हुआ है?

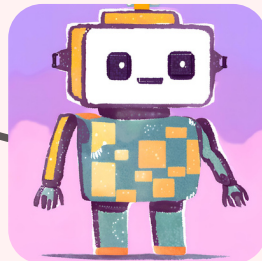


अरे, इंटरनेट! यह वाकई एक शानदार चीज़ है, लेकिन बहुत कम ही लोग कि इस बारे में सोचते हैं कि ये कैसे काम करता है। चलो, इसे मिलकर समझते हैं! इसके लिए मैं इन चीज़ों को समझाने में माहिर किसी को लाता हूँ!

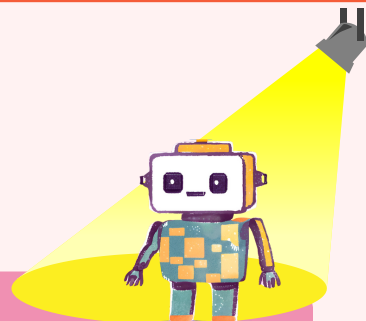


अमित भैया के फ़ोन पर टैप करते ही, एक छोटा सा रोबोट कमरे में आ गया। उसमें चमकदार रोशनी और एक खुशनुमा बीप थी।

हेलो, मीरा! मैं ग्लिच हूँ, तुम्हारा ऑनलाइन दोस्त! मैं यहाँ तुम्हारी मदद करने के लिए हूँ ताकि तुम इंटरनेट की विशाल दुनिया को अच्छे से जान सको।



# इंटरनेट क्या है?



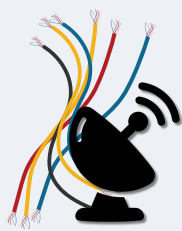
आइए बुनियादी चीजों से शुरुआत करें, इंटरनेट एक बहुत बड़े जाल की तरह है जो दुनिया भर के अरबों कंप्यूटर, फोन और डिवाइस को जोड़ता है। ये कनेक्शन डिवाइस को जानकारी का आदान-प्रदान करने में मदद करते हैं, जिससे आपके लिए ब्राउज़ करना, वीडियो देखना, गेम खेलना और यहां तक कि ऑनलाइन खरीदारी करना भी संभव हो जाता है।



कल्पना कीजिए कि इंटरनेट हमारी व्यस्त भारतीय रेल की तरह है। जैसे रेलगाड़ियाँ दिल्ली, मुंबई, चेन्नई, कोलकाता और कई अन्य शहरों के बीच लोगों और सामान को ले जाती हैं, वैसे ही इंटरनेट भी दुनिया भर में सूचनाएँ पहुँचाता है।

हर वेबसाइट का अपना एक पता होता है, जैसे हर रेलवे स्टेशन का अपना नाम होता है! फर्क बस इतना है कि जहाँ ट्रेन को लोगों और सामान को एक जगह से दूसरी जगह ले जाने में घंटों और दिन लग जाते हैं, वहीं इंटरनेट को जानकारी पहुँचाने में सिर्फ़ कुछ सेकंड लगते हैं।

## रीढ़ की हड्डी



इंटरनेट दुनिया भर के उपकरणों को जोड़ने के लिए बड़े-बड़े भूमिगत केबलों, उपग्रहों और वायरलेस नेटवर्क पर निर्भर करता है।

## सर्वर



यह एक सर्वर है, जो आपके द्वारा ऑनलाइन देखी गई जानकारी को स्टोर करता है। सर्वर लाखों वेबसाइटों, वीडियो और ऐप्स के साथ विशाल लाइब्रेरी की तरह होते हैं।

## आपका ब्राउज़र

Search



जब आप अपने ब्राउज़र में कोई सवाल टाइप करते हैं, तो आपका डिवाइस सर्वर को एक रिक्वेस्ट भेजता है। सर्वर जवाब खोजता है और कुछ ही सेकंड में आपको वापस भेज देता है!

# इंटरनेट हमें किस तरह मदद करता है?

इंटरनेट ने हमारे जीवन और सीखने के तरीके में एक बड़ा बदलाव ला दिया है। चलिए, मैं आपको बताता हूँ कि यह हमारे दैनिक जीवन में कैसे हमारी मदद करता है।



## सीखना और शिक्षा

इंटरनेट आपके लिए एक शिक्षक और लाइब्रेरी दोनों की तरह है! सीखने के प्लेटफॉर्म तक पहुंचें, किसी भी भाषा में वीडियो देखें और अपने पसंदीदा विषयों के बारे में जानने के लिए वर्चुअल क्लासरूम में शामिल हों - सब कुछ बस एक क्लिक से।



## संचार

तुरंत जुड़े! चाहे ईमेल हो, सोशल मीडिया, मैसेजिंग ऐप या वीडियो कॉल, इंटरनेट संचार को तेज़, आसान और सहज बनाता है।



## मनोरंजन

इंटरनेट आपके मनोरंजन का एक साधन है - घर पर आराम से फिल्में देखें, क्रिकेट मैच देखें, गेम खेलें या डांस जैसे नए कौशल सीखें।



## रचनात्मकता और साझा करना

अपनी रचनात्मकता को दुनिया के साथ बांटें! कहानियाँ लिखें, संगीत बनाएं, या ऑनलाइन अपनी कलाकृतियाँ दिखाएं, जैसे कि कई प्रतिभाशाली युवा कलाकार हर दिन करते हैं।

भैया, मैंने ऑनलाइन कक्षाओं के लिए इंटरनेट का इस्तेमाल करना शुरू कर दिया है, और अब, मुझे पढ़ाई के बाद आराम करने के लिए मजेदार वीडियो देखना और ऑनलाइन गेम खेलना बहुत पसंद है! लेकिन मुझे नहीं पता था कि मैं ऑनलाइन नृत्य या संगीत भी सीख सकता हूँ!



अरे वाह यह तो शानदार है! लेकिन तुम अकेली नहीं हो: तुम जैसे 88% युवा भारतीय ऑनलाइन वीडियोस देखते हैं। कई लोग गेमिंग, जानकारी खोजने और दोस्तों से बात करने के लिए इंटरनेट का इस्तेमाल करते हैं! और बहुत से युवा ऑनलाइन नई-नई चीजें खोज रहे हैं- क्या यह कमाल नहीं है?!

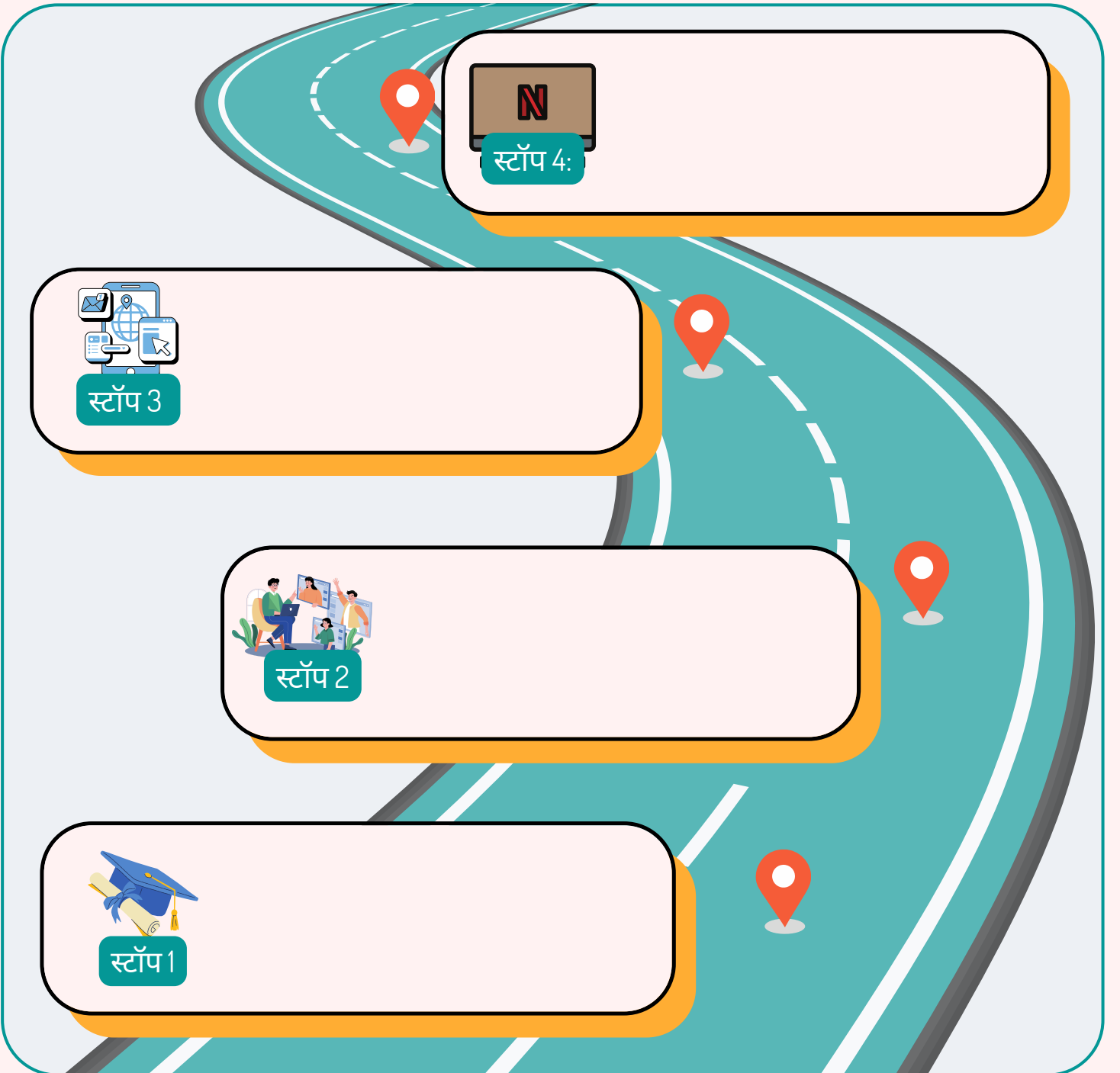


## गतिविधि



इंटरनेट की नई समझ के साथ, मीरा इसकी अनंत संभावनाओं को खोजने के लिए तैयार महसूस कर रही थी। अगर आपने कभी इंटरनेट का इस्तेमाल किया है, तो अपने ऑनलाइन अनुभवों को साझा करके मीरा को नई चीजें खोजने में मदद करें। नीचे से शुरू करें, और

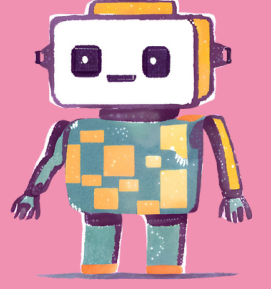
- स्टॉप 1 पर, ऑनलाइन सीखी गई किसी नई चीज के बारे में सोचें।
- स्टॉप 2 पर आपके द्वारा बनाई गई या साझा की गई कोई रचनात्मक चीज बताएं।
- स्टॉप 3 जुड़े रहने के लिए है—आप ऑनलाइन किससे संपर्क में रहते हैं?
- स्टॉप 4 पूरी तरह से मौज-मस्ती के बारे में है—आपकी पसंदीदा ऑनलाइन गतिविधि क्या है?



इंटरनेट केवल वर्तमान के बारे में नहीं है। यह हमेशा बदलता रहता है, और आप इसके भविष्य का हिस्सा हैं।



भारत में हम पहले से ही बड़े बदलाव देख रहे हैं। आप या आपके माता-पिता शायद UPI या यूनिकाइड पेमेंट्स इंटरफ़ेस का इस्तेमाल कर रहे हैं! UPI हमें डिजिटल तरीके से पैसे भेजने और लेने की सुविधा देता है, जिससे हमारी अर्थव्यवस्था में बदलाव आ रहा है। कई नई सेवाएँ ऑनलाइन भी उपलब्ध हैं—जैसे कि डॉक्टर वीडियो कॉल के जरिए मरीजों का इलाज कर रहे हैं और छात्र घर से ही कक्षाओं में शामिल हो रहे हैं।



आर्टिफिशियल इंटेलिजेंस, जिसे हम AI कहते हैं, इंटरनेट को और भी स्मार्ट बना रहा है। AI मशीनों को इंसानों की तरह सोचने और सीखने की क्षमता देता है। AI टूल्स लोगों के सवालों के जवाब दे सकते हैं, हर व्यक्ति के हिसाब से शिक्षा को बेहतर बना सकते हैं, गेम्स को ज़्यादा रोमांचक बना सकते हैं, और डेटा के आधार पर समस्याओं की पहचान करने में मदद कर सकते हैं।

अब वर्चुअल रियलिटी या VR हमारे जीवन में है, एक ऐसी तकनीक जो खुद एक नया वातावरण तैयार करती है और लोगों को हेडसेट के जरिए उस वातावरण के साथ इंटरैक्ट करने का मौका देती है। सोचिए, आप एक खूबसूरत जंगल में टहल रहे हैं, ताजमहल की खूबसूरती देख रहे हैं, या फिर अंतरिक्ष की सैर कर रहे हैं - ये सब अपने कमरे से!

धन्यवाद, भैया और ग्लिच! मुझे नहीं पता था कि इंटरनेट इतना ज़बरदस्त और शक्तिशाली है। अब मैं इंटरनेट पर बहुत कुछ नया सीखने और जानने के लिए बहुत उत्साहित हूँ!



मैं भी तुम्हारे लिए उत्साहित हूँ! लेकिन जैसे-जैसे इंटरनेट बदलता है, तुम तरह-तरह के अनुभवों से गुज़रोगी—कुछ अच्छे, तो कुछ बुरे। मैं चाहता हूँ कि तुम इसके लिए तैयार रहो।



## गतिविधि

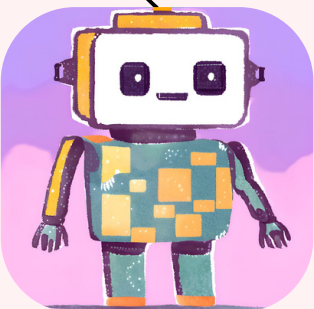


मीरा चुपचाप अपने कमरे में बैठी रही और अमित भैया की बात के बारे में सोचती रही। उसे इंटरनेट बहुत पसंद था, लेकिन अमित भैया की बात सही थी: तैयार रहना ज़रूरी है। वो उन सभी पलों के बारे में सोचने लगी जब उसे इंटरनेट एक अच्छी जगह नहीं लगा, और उसने एक सूची बनाना शुरू किया। क्या आपके साथ भी मीरा जैसा कोई अनुभव हुआ है? अपनी खुद की सूची बनाइए:



मुझे इंटरनेट पसंद नहीं आता जब...

- लोग दूसरों को डराने के लिए गलत जानकारी फैलाते हैं।
- दूसरे लोग मुझ पर कुछ करने के लिए दबाव डालने की कोशिश करते हैं।
- कोई मुझसे ऑनलाइन झूठ बोलता है या बुरा व्यवहार करता है।
- मुझे बहुत सारी जानकारी मिलती है, इससे मैं परेशान हो जाती हूँ।
- मुझे अनचाहे मैसेज मिलते हैं या ऐसे वीडियो दिखते हैं जो मुझे पसंद नहीं आते।
- कोई मुझसे धोखे से पैसे निकलवाने की कोशिश करता है और मुझे असुरक्षित महसूस कराता है!



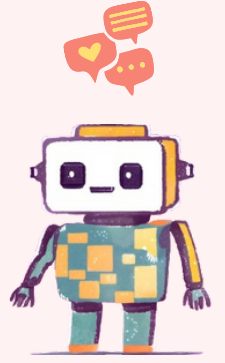
बुरे ऑनलाइन अनुभवों के बारे में सोचना कभी-कभी मुश्किल हो सकता है, लेकिन यह मददगार भी हो सकता है। सोचिए कि जब आपको ऐसा महसूस हुआ तो क्या हुआ? याद रखें, आप अकेले नहीं हैं - ऑनलाइन और ऑफलाइन दोनों जगह परेशान करने वाली भावनाएँ जैसे परेशानी, गुस्सा या उदासी होना सामान्य है। चलिए, असुरक्षित स्थितियों की पहचान करने के लिए एक साथ काम करते हैं और सीखते हैं कि ऑनलाइन खुद की देखभाल कैसे करें।

सुरक्षित इंटरनेट उपयोग की पहली सीढ़ी है इंटरनेट को अच्छे से समझना और नई जानकारी से खुद को अपडेट रखना। यहाँ कुछ ज़रूरी बातें हैं, जो ऑनलाइन रहते समय ध्यान में रखनी चाहिए।

सबसे पहले — आपका डिजिटल फुटप्रिंट। आपका डिजिटल फुटप्रिंट उस चिह्न की तरह है जो आप ऑनलाइन रहते समय छोड़ते हैं। चाहे वह आपके द्वारा शेयर की गई पोस्ट हो, आपके द्वारा अपलोड की गई तस्वीर हो या फिर आपके द्वारा सर्च की गई कोई चीज़, ये सब आपकी डिजिटल पहचान का हिस्सा बनते हैं।



रुको! क्या इसका मतलब है कि मेरी सर्च हिस्ट्री भी मेरे डिजिटल फुटप्रिंट का हिस्सा है? अगर मैं गुप्त मोड का इस्तेमाल करती हूँ तो क्या होगा? यकीनन कोई भी मेरे डिजिटल फुटप्रिंट को ट्रैक नहीं कर सकता!



हर क्लिक, लाइक और शेयर से आपकी ऑनलाइन पहचान बनती है। इसे ऐसे समझो – जैसे आप अपने मोहल्ले में एक भेष बदलकर घूम रहे हों। आपके दोस्त शायद आपको न पहचानें, लेकिन सुरक्षा गार्ड, दुकानदार या कैमरे फिर भी देख सकते हैं कि आप कहाँ जा रहे हैं और क्या कर रहे हैं। आपके ब्राउज़र का इन्कोग्निटो मोड भी इसी तरह काम करता है। यह कुछ चीज़ें छिपा सकता है, जैसे कि आपके कंप्यूटर या फोन को इस्तेमाल करने वाले दूसरे लोग यह न देख सकें कि आपने कौन-कौन सी वेबसाइट खोलीं। लेकिन यह आपको पूरी तरह से अदृश्य नहीं बनाता। क्या आप जानना चाहते हैं कि फिर भी कौन आपकी ऑनलाइन गतिविधियों को देख सकता है?



आपका वाई-फ़ाई या इंटरनेट प्रोवाइडर (जो कंपनी आपको इंटरनेट देती है) यह देख सकता है कि आप कौन-कौन सी वेबसाइट विज़िट कर रहे हैं। इसे ऐसे समझो – जैसे कोई दुकानदार यह जान सकता है कि आप उसकी दुकान में आए थे, भले ही वह आपके भेष को न पहचान पाए।



कई वेबसाइटें आपके बारे में जानकारी रखने के लिए कुकीज़ या ट्रैकर्स जैसे टूल का उपयोग करती हैं। हालांकि, जब आप ब्राउज़र बंद करते हैं, तो गुप्त मोड उन्हें हटा देता है। लेकिन अगर आप लॉग इन करते हैं या वेबसाइट आपके डिवाइस को पहचानती है, तो उसे यह पता चल सकता है कि आपने कहाँ-कहाँ विज़िट किया।

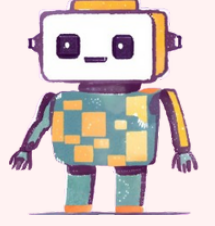


कई बार स्कूल या ऑफिस में वाई-फ़ाई के जरिए इंटरनेट इस्तेमाल पर नजर रखने के लिए कुछ टूल्स होते हैं, यहां तक कि गुप्त मोड में भी।

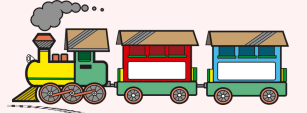
वाह, मुझे तो पता ही नहीं चला कि जो कुछ भी मैं करती हूँ, वो कहीं न कहीं रिकॉर्ड हो रहा है। मैंने ये भी देखा है कि हर वेबसाइट मुझसे उनका इस्तेमाल करने से पहले मेरा नाम, फोन नंबर, स्थान या ईमेल आईडी मांगती है! मुझे और क्या याद रखना चाहिए?



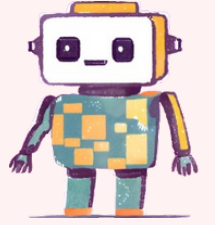
मैं तुमसे दो कदम आगे हूँ! चलो इंटरनेट के बारे में कुछ दिलचस्प और थोड़ी-बहुत गुप्त बातें समझते हैं। क्या तुमने कभी ध्यान दिया है कि तुम जो कुछ भी खोजती हो, उसके लिए विज्ञापन कैसे अचानक सामने आ जाते हैं, या तुम्हारे सोशल मीडिया फ़ीड में हमेशा वही वीडियो क्यों होते हैं जो तुम्हें पसंद आते हैं? ये सब एल्गोरिदम और कुकीज़ की वजह से होता है!



मेरी चचेरी बहन ने एक बार शैंपू के बारे में खोज की और जब वह अगली बार ऑनलाइन गई, तो उसे शैंपू एड के लिंक लगातार दिखते रहे। हमें लगा कि यह बस एक संयोग है! एल्गोरिदम कैसे काम करते हैं?



यह कुछ हद तक रेलवे सिस्टम जैसा है। सोचिए, जब आप किसी वेबसाइट पर जाते हैं, तो वो एक स्टेशन है, और जो भी काम आप करते हैं, जैसे कि कोई पोस्ट लाइक करना, कुछ खोजना या अपनी कार्ट में कोई आइटम जोड़ना - वो उस स्टेशन से निकलने वाली ट्रेन है। एल्गोरिदम ट्रेन कंडक्टर की तरह होते हैं। वे देखते हैं कि आपकी ट्रेनें कहाँ जा रही हैं और आपकी पिछली यात्राओं के आधार पर आपके अगले स्टेशन का पता लगाने की कोशिश करते हैं। अगर आप वीडियो गेम से जुड़े कई स्टेशनों पर जाते हैं, तो एल्गोरिदम को लगता है कि आपको गेमिंग पसंद है और वे आपको विज्ञापन भेज सकते हैं या गेमिंग से जुड़ी सामग्री सुझा सकते हैं।

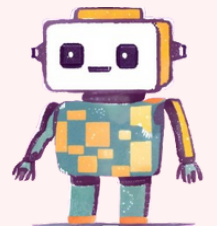


दूसरी ओर, कुकीज़ स्टेशन के टिकट की तरह होती हैं जो आपके डिवाइस पर रहती हैं ताकि वेबसाइट को पता चले कि आप पहले भी वहाँ गए हैं। आप उन्हें हटा सकते हैं और टिकट को फेंक सकते हैं। याद रखें, हर यात्रा एक निशान छोड़ जाती है!

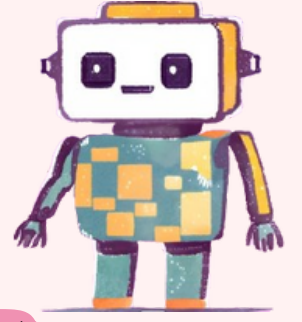
अगर मैं किसी उपनाम का इस्तेमाल करूँ तो क्या होगा?



यह एक शानदार सवाल है! चलो गुमनामी के बारे में चर्चा करते हैं। इंटरनेट पर, लोग अक्सर अपनी असली पहचान नहीं बताते।



कभी-कभी, लोग मजे करने, सुरक्षित महसूस करने या अपने व्यक्तित्व को समझने के लिए अपने असली नाम और तस्वीरों के अलावा अलग-अलग यूजरनेम और तस्वीरें इस्तेमाल करते हैं। यह ठीक है, लेकिन गुमनामी की अपनी सीमाएं हैं: किसी की ऑनलाइन गतिविधियों का अभी भी किसी न किसी तरीके से पता लगाया जा सकता है, क्योंकि... आपने सही सोचा... आपके डिजिटल ट्रेस!

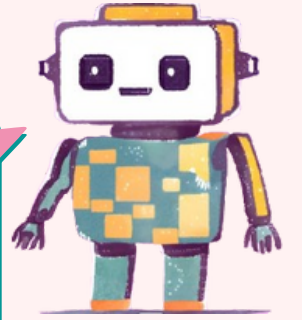


और ये भी ध्यान रखें, लोग दूसरों को नुकसान पहुंचाने के लिए अपनी पहचान छिपा सकते हैं या अपने बारे में झूठ बोल सकते हैं। हर कोई वैसा नहीं होता जैसा वो दिखता है।

मैं आमतौर पर उन दोस्तों से ऑनलाइन बात करता हूँ जिन्हें मैं जानता हूँ और जिन पर मुझे भरोसा है! वो भी अपनी माँ के अकाउंट का इस्तेमाल करके।



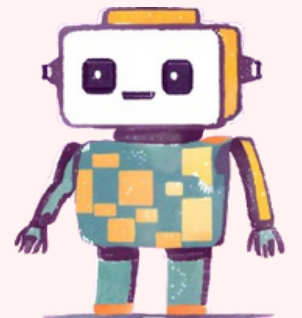
आह! तो आपको अलग-अलग ऑनलाइन स्पेस के बारे में कुछ बातें जाननी चाहिए। जैसे, आपका ग्रुप चैट एक प्राइवेट स्पेस है। आप वहाँ एक पदचिह्न छोड़ते हैं, लेकिन यह समूह के बाहर के लोगों को नहीं दिखता। ऑनलाइन और भी जगहें हैं जहाँ आपकी पोस्ट सभी को दिखाई दे सकती हैं- जैसे किसी पब्लिक अकाउंट से किया गया ट्वीट! हमेशा इस बात का ध्यान रखें कि आपके संदेश, पोस्ट और लाइक कौन देख सकता है। बाद में, हम सीखेंगे कि इसे कैसे बदला जा सकता है!



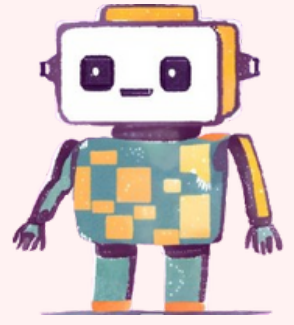
धन्यवाद ग्लिच! आज मैंने बहुत कुछ सीखा, लेकिन यह मुझे थोड़ी चिंता में डाल रहा है।



हमारे ऑनलाइन और ऑफलाइन जीवन में, हमें सकारात्मक और नकारात्मक दोनों तरह के अनुभवों का सामना करना पड़ सकता है। इंटरनेट के बारे में जानकारी हासिल करके और दोस्तों या भरोसेमंद वयस्कों के साथ साझा करके, आप समझदारी से विकल्प चुन सकते हैं और इसके फायदों का आनंद ले सकते हैं। यह तो बस शुरुआत है! जितना अधिक आप सीखेंगे, उतना ही अधिक शक्तिशाली महसूस करेंगे।



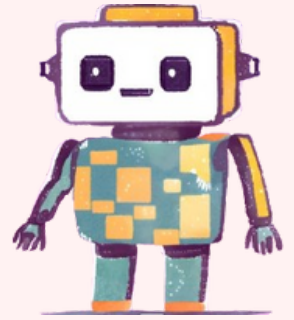
तब तक, क्या आप इंटरनेट के बारे में अपनी तीन इच्छाएँ हमारे साथ साझा कर सकते हैं? चलो देखते हैं कि क्या हम उन्हें पूरा कर सकते हैं!



हाहा, बिलकुल सही! मैं ऑनलाइन तकनीक के बारे में और जानकारी हासिल करना चाहता हूँ। मैं चाहता हूँ कि इंटरनेट हर किसी के लिए एक सुरक्षित स्थान बने... और मैं चाहता हूँ... मैं चाहता हूँ कि मैं नए-नए ऐप्स को लगातार आजमाता रहूँ!



अरे, इंटरनेट के लिए आपकी क्या इच्छाएँ हैं? मुझे बताओ!



## गतिविधि

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



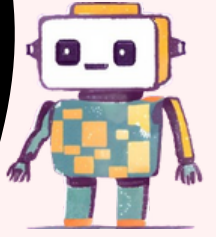


## क्या आप जानते हैं ?

आजकल रोज़ मैं इतनी सारी वेबसाइट्स देखती हूँ। मैं कभी कभी सोचती हूँ कि दुनिया की पहली वेबसाइट कौनसी होगी।



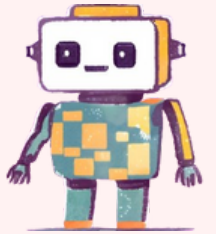
दुनिया की पहली वेबसाइट 1989 में बनाई गई थी। इसका नाम "info.cern.ch" था। ज़रा सोचो, 1989 में इंटरनेट का इस्तेमाल करना कैसा रहा होगा-यह आज की रंग-बिरंगी और इंटरैक्टिव वेबसाइटों से बहुत अलग था। क्या आप उस वैज्ञानिक का नाम बता सकते हैं जिसने पहली वेबसाइट बनाई थी?



और क्या तुम जानते हो कि आज की तारीख में कितनी वेबसाइट्स हैं?



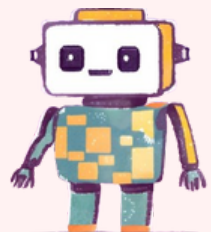
इंटरनेट एक बहुत बड़ी लाइब्रेरी की तरह है, जहाँ हमारे देखने के लिए अनगिनत किताबें मौजूद हैं। अभी इंटरनेट पर ॥ अरब से ज्यादा वेबसाइटें हैं, और यह संख्या हर दिन बढ़ रही है! लेकिन घबराने की जरूरत नहीं-इनमें से कई वेबसाइटें डिजिटल म्यूज़ियम की तरह हैं, जहाँ हमें कीमती ज्ञान और मनोरंजन मिल सकता है।



अगर इंटरनेट पर इतनी सारी जानकारी स्टोर्ड है, तो क्या इसका वजन बहुत ज्यादा होगा?



यह सुनकर यकीन करना मुश्किल है, लेकिन पूरा इंटरनेट लगभग 60 ग्राम वजन का है! यह एक स्ट्रॉबेरी के वजन के बराबर है! 🤖 क्या आप अंदाजा लगा सकते हैं क्यों? दरअसल, जानकारी का भी अपना वज़न होता है, भले ही हम उसे देख नहीं सकते!



## रिक्वैप : हैलो डिजिटल दुनिया!



इंटरनेट एक विशाल जाल की तरह है जो दुनिया भर के उपकरणों को जोड़ता है और हमें संवाद करने, सीखने और खोज करने की सुविधा देता है।



ऑनलाइन प्लेटफॉर्म कुकीज़ और कैश के माध्यम से आपकी गतिविधियों पर नज़र रखते हैं, जिससे आपकी निजी आदतें और जानकारी उजागर हो सकती हैं।



ऑनलाइन की गई हर क्रिया एक डिजिटल निशान छोड़ती है, इसलिए हमेशा सोच-समझकर जानकारी साझा करें।



हमेशा अपनी निजी जानकारी के प्रति सतर्क रहें। जो जानकारी आप साझा करते हैं, उसे एक्सेस किया जा सकता है और स्टोर किया जा सकता है।



# चैप्टर 2: स्कैम्स, हैक्स और साइबर हमले: होशियार रहो!



आज मीरा का जन्मदिन है! उसका घर हंसी-मज़ाक और स्वादिष्ट खाने की खुशबू से भरा हुआ है। उसकी माँ ने रहीम और उसके परिवार को रात के खाने के लिए बुलाया है। जैसे ही रहीम का परिवार आता है, बड़े लोग ड्राइंग रूम में बैठकर कहानियाँ सुनाने लगते हैं और बातें करते हैं। इस बीच, मीरा खुशी-खुशी रहीम को अपने कमरे में ले जाती है और अपना नया फ़ोन दिखाती है।



देखो, रहीम! मेरे मम्मी-पापा ने आखिरकार मुझे मेरा खुद का फोन दिला दिया! अब मैं वो सारे गेम और ऐप डाउनलोड कर सकती हूँ जो मैं चाहती थी!

यह बहुत अच्छा है, मीरा! डाउनलोड शुरू करने से पहले, तुम्हें पहले एक ईमेल आईडी और पासवर्ड बनाना होगा। चलो, इसे करते हैं!



मीरा जल्दी से अपना ईमेल आईडी iammeera@gmail.com टाइप करती है और गर्व से मुस्कुराते हुए अपना पासवर्ड IAMMEERA सेट करती है। तभी ग्लिच अचानक प्रकट होता है और उसे चेतावनी देता है!



ईमेल आईडी

iammeera@gmail.com

पासवर्ड:

IAMMEERA



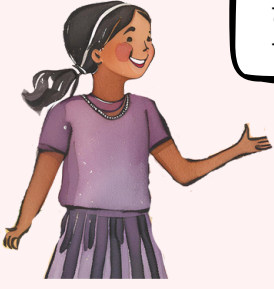
कमज़ोर पासवर्ड! सुरक्षा खतरे में!



इस पासवर्ड में क्या समस्या है? इसे याद करना तो आसान है। मेरी माँ के फ़ोन में हमेशा इतने लंबे और जटिल पासवर्ड होते थे कि मैं कभी भी उन्हें याद नहीं रख पाती थी। मुझे हर बार लॉग इन करने के लिए उन्हें परेशान करना पड़ता था।



आसान पासवर्ड हमेशा जोखिम भरे होते हैं, है ना? जरा सोचो: अगर कोई आपके बारे में जानता है और आपके अकाउंट तक पहुंचना चाहता है, तो वह सबसे पहले आपका नाम या कोई पसंदीदा वाक्यांश आजमाएगा! लेकिन अगर पासवर्ड थोड़ा जटिल और अनोखा है, तो यह एक कठिन पहली की तरह हो जाएगा - न तो इंसान और न ही मशीनें इसे आसानी से सुलझा पाएंगी। चलो फिर से कोशिश करते रहें।



यह सच में मददगार है! चलो इसे आजमाते हैं:  
M3eRa!sB1rthd@y  
वाह! यह सच में काम कर गया! अब मैं अपने सभी अकाउंट के लिए इसका उपयोग करूंगी।

नहीं! अमित भैया ने कहा था कि हर अकाउंट के लिए एक ही पासवर्ड का इस्तेमाल करना आपके घर, कार और लॉकर के लिए एक ही चाबी का इस्तेमाल करने जैसा है। अगर किसी को यह मिल जाए, तो वह सब कुछ अनलॉक कर सकता है। अगर एक ऐप हैक हो जाता है - तो आपका पासवर्ड गलत हाथों में जा सकता है, और आपके सभी दूसरे अकाउंट खतरे में पड़ सकते हैं।



अरे नहीं! मैंने इस बारे में नहीं सोचा। मुझे अब क्या करना चाहिए?



हर एक अकाउंट के लिए एक खास पासवर्ड का उपयोग करना बेहतर है!



इतने सारे पासवर्ड्स याद रखना थोड़ा मुश्किल होगा। अच्छा होगा कि मैं इन्हें अपनी डायरी में लिख लूँ!



मैंने भी यही सोचा था, लेकिन फिर मैंने पासवर्ड मैनेजर का इस्तेमाल करना शुरू कर दिया। यह सच में बहुत मददगार है! अब मुझे सिर्फ एक मजबूत मास्टर पासवर्ड याद रखना है और मैं अपने सभी दूसरे पासवर्ड देख सकता हूँ। अगर कोई मेरा पासवर्ड चुराने की कोशिश भी करता है, तो मैंने 2-फैक्टर ऑथेंटिकेशन चालू कर रखा है, इसलिए वे मुझे नहीं पकड़ सकते! यह आपके डिजिटल दरवाजे पर एक और ताला लगाने जैसा है, हाहा!



ओह! मुझे लगा था कि एक मजबूत पासवर्ड ही काफी होगा, लेकिन अब मुझे लगता है कि हमें और भी सुरक्षा अपनाने की जरूरत है!



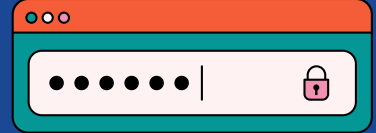
सुरक्षा की कई परतें होना हमेशा फायदेमंद होता है। ऐप्लिकेशन लॉक चेक करना मत भूलिए! अब चलो चलें— केक काटने का समय हो गया है ना? मुझे तो बहुत भूख लगी है!










आइए मीरा के अनुभव से सीखें और यह सुनिश्चित करें कि आपके खाते की सुरक्षा शुरू से ही हो। जब आप किसी नए एप्लिकेशन के लिए साइन अप कर रहे हों या खाता बना रहे हों, तो एक मजबूत पासवर्ड बनाने के लिए इन महत्वपूर्ण दिशा-निर्देशों का पालन करें:

## मजबूत पासवर्ड की चेकलिस्ट



-  **अक्षरों का मिश्रण इस्तेमाल करें:** बड़े अक्षरों (ABC) और छोटे अक्षरों (abc), संख्याओं और विशेष प्रतीकों (जैसे, @, #, \$, !) को मिलाकर उपयोग करें। इससे हैकर्स के लिए आपके पासवर्ड का अनुमान लगाना बहुत मुश्किल हो जाता है।
-  **इसे लंबा बनाएं:** और अधिक सुरक्षा के लिए, पासवर्ड को कम से कम 12 से 16 अक्षरों का होना चाहिए। लंबे पासवर्ड को तोड़ने में काफी समय लगता है, मजबूत टूल का उपयोग करने पर भी।
-  **सामान्य शब्दों और वाक्यांशों से बचें:** ऐसे शब्दों का उपयोग न करें जो आसानी से अनुमान लगाए जा सकें, जैसे "पासवर्ड", "123456" या कोई भी व्यक्तिगत जानकारी जिसे बहुत से लोग जानते हों, जैसे आपका नाम, पालतू जानवर का नाम या पसंदीदा वाक्यांश।
-  **स्पष्ट व्यक्तिगत जानकारी से बचें:** जन्मदिन, सालगिरह या फोन नंबर जैसी जानकारी अक्सर सोशल मीडिया के माध्यम से सार्वजनिक रूप से उपलब्ध होती है, तो इन्हें पासवर्ड के रूप में इस्तेमाल नहीं किया जाना चाहिए।
-  **पासफ्रेज़ पर ध्यान दें:** आप एक यादगार वाक्य या वाक्यांश का इस्तेमाल कर सकते हैं और उसमें कुछ बदलाव करके उसे और जटिल बना सकते हैं। जैसे, "I love icecream" को "iL0v3!c3Cr34m@2024" में बदल सकते हैं।

### इसका महत्व क्या है?

आज की दुनिया में, हममें से कई लोग सोशल मीडिया, ईमेल और बैंकिंग जैसे कई अकाउंट्स संभालते हैं। एक मजबूत पासवर्ड आपकी सुरक्षा की पहली ढाल होती है, जो किसी को बिना इजाज़त आपके अकाउंट में घुसने से रोकती है। अगर पासवर्ड कमज़ोर या बार-बार इस्तेमाल किया हुआ हो, तो आपका डेटा चोरी हो सकता है, आर्थिक नुकसान हो सकता है, या आपकी पहचान का गलत इस्तेमाल किया जा सकता है। हम इस चैप्टर में इन खतरों और बाकी जरूरी बातों को विस्तार से समझेंगे। जैसे-जैसे हैकर्स और चालाक होते जा रहे हैं, इन सुरक्षा उपायों को अपनाना आपके अकाउंट्स की सुरक्षा को काफी मजबूत बना सकता है।



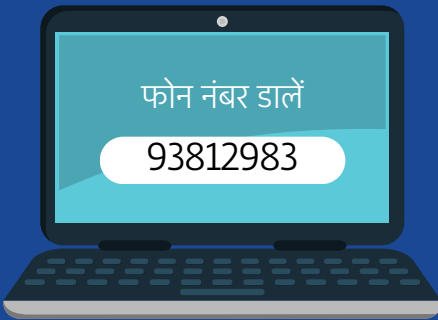
## 2 फैक्टर ऑथेंटिकेशन

टू-फैक्टर ऑथेंटिकेशन (2FA) आपके अकाउंट के लिए एक अतिरिक्त सुरक्षा परत है। कई पॉपुलर प्लेटफॉर्म इसे इस्तेमाल करने की सलाह देते हैं। जब आप इस फीचर को ऑन करते हैं, तो पासवर्ड डालने के बाद भी लॉगिन के लिए एक और वेरिफिकेशन की जरूरत होती है। अक्सर, यह एक वन-टाइम पासवर्ड (OTP) होता है, जो आपके पर्सनल मोबाइल नंबर पर भेजा जाता है। यह पासकी, ईमेल या फिंगरप्रिंट स्कैन भी हो सकता है। OTP कुछ ही मिनटों के लिए वैध रहता है और सिर्फ एक बार इस्तेमाल किया जा सकता है। अगली बार लॉगिन करने के लिए आपको फिर से नया कोड दर्ज करना होगा।



### यह कैसा नजर आता है:

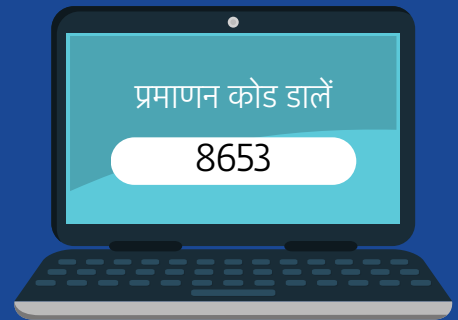
उपयोगकर्ता फोन नंबर भरता है



उपयोगकर्ता को एक बार का पासवर्ड (OTP) मिलता है।



उपयोगकर्ता OTP डालता है।



### कैसे सेट करें:

1. नेविगेशन पैनल में जाएँ। आप ये आइकन देख सकते हैं:



1. सेटिंग्स के विकल्प पर जाएँ। यह आमतौर पर कुछ इस तरह नजर आता है:



1. अब 'सुरक्षा' या 'गोपनीयता' जैसा कोई बटन खोजें।

## अकाउंट सेटिंग्स

निजी सुरक्षा सूचनाएं

खाता की सुरक्षा  
आपके खाते की सुरक्षा में मदद करने के लिए सेटिंग्स

पासवर्ड को बदलें  
अपने खाते की सुरक्षा के लिए एक खास पासवर्ड चुनें।

2 कारक प्रमाणीकरण  
अपनी पहचान को सत्यापित करने के लिए इसे सक्रिय करें।

1.4. टू-फैक्टर ऑथेंटिकेशन ऑन करें। आपको वेरिफिकेशन के कुछ ऑप्शन्स दिखाएंगे। आप SMS, ऐप या फिंगरप्रिंट में से कोई भी तरीका चुन सकते हैं।

## दो-कारक प्रमाणीकरण सेट करें

1 विधि का चयन करें

2 सत्यापन करें

3 बैकअप डालें

### प्रमाणीकरण की विधि चुनें

अपने यूजरनेम और पासवर्ड के अलावा, आपको एक और पासवर्ड डालना होगा।  
अपने खाते में लॉग इन करने के लिए अपना ईमेल पता डालें (जो एप्लिकेशन या एसएमएस के जरिए भेजा जाएगा)।

प्रमाणन ऐप  
किसी ऐप से कोड लें

एसएमएस  
एसएमएस के जरिए एक खास कोड पाएं

ईमेल आईडी  
ईमेल के जरिए एक खास कोड पाएं

# पासवर्ड मैनेजर



## • पासवर्ड मैनेजर का काम क्या होता है?

1. पासवर्ड को सुरक्षित रखें: पासवर्ड मैनेजर एक डिजिटल लॉकर की तरह होता है, जो आपके पासवर्ड को सुरक्षित रखते हैं।
2. मजबूत पासवर्ड बनाएं: आप हर खाते के लिए नया और मजबूत पासवर्ड बना सकते हैं, जिससे यह सुनिश्चित होता है कि आप कमजोर या अनुमानित पासवर्ड का फिर से उपयोग न करें।
3. अपने आप क्रेडेंशियल भरें: कई पासवर्ड मैनेजर अपने आप आपके लॉगिन डिटेल्स भर देते हैं, जिससे आपका समय बचता है।



## • पासवर्ड मैनेजर का इस्तेमाल क्यों करें?



पासवर्ड मैनेजर के साथ, आपको कई जटिल पासवर्ड याद रखने की जरूरत नहीं पड़ेगी - बस एक बहुत ही मजबूत मास्टर पासवर्ड जो आपके पासवर्ड मैनेजर को अनलॉक करता है। अब आपको अपने सभी पासवर्ड याद रखने की चिंता नहीं करनी पड़ेगी, और न ही पासवर्ड रीसेट करने में कोई परेशानी होगी!



पासवर्ड मैनेजर यह सुनिश्चित करता है कि आपका डेटा मजबूत एन्क्रिप्शन के साथ सुरक्षित हो, जैसे एक गुप्त कोड जिसे केवल आप अपने मास्टर पासवर्ड का उपयोग करके ही तोड़ सकते हैं। इसके बिना, हैकर्स के लिए आपके पासवर्ड तक पहुंच पाना असंभव है!



कुछ पासवर्ड मैनेजर फर्जी वेबसाइटों और ऑनलाइन खतरों को पहचानने में मदद कर सकते हैं। ये आपको धोखाधड़ी वाले पेजों पर गलती से अपने क्रेडेंशियल डालने से रोकते हैं। क्या यह शानदार नहीं है?

# एप्लिकेशन लाक्स



कल रहीम मेरे पास एक दिलचस्प समस्या लेकर आया। उसे कॉलोनी में अपने दोस्तों को स्मार्टफोन का इस्तेमाल करना सिखाना बहुत पसंद है। लेकिन, उसके फोन में कुछ संवेदनशील जानकारी है, जैसे निजी नोट्स, दोस्तों और परिवार के साथ की तस्वीरें, और निजी मैसेजएस। वह अपने फोन को दूसरों को सीखने के लिए देना चाहता है, लेकिन उसे यह सुनिश्चित करना है कि उसकी गोपनीयता और सुरक्षा बची रहे। मैंने उसे सलाह दी: ऐप लॉक का इस्तेमाल करो!

ऐप लॉक पासवर्ड, पिन या बायोमेट्रिक एक्सेस की मदद से फोन में खास एप्लिकेशन्स की सुरक्षा को बढ़ाता है। यहां बताया गया है कि कोई अपने फोन को सुरक्षित तरीके से कैसे दूसरों के साथ साझा कर सकता है:



ऐप लॉक को डाउनलोड करें



सुरक्षित पिन बनाएं



लॉक करने के लिए ऐप चुनें



बायोमेट्रिक प्रमाणीकरण चालू करें

## ऐप लॉक के फायदे

- गोपनीयता की सुरक्षा: रहीम की संवेदनशील जानकारी सुरक्षित रहती है, भले ही कोई और उसका फोन इस्तेमाल कर रहा हो।
- अपनी पसंद से सेट करें: वह खुद तय कर सकता है कि किन ऐप्स को लॉक करना है।
- आसान इस्तेमाल: एक बार सेट करने के बाद, ऐप लॉक का इस्तेमाल करना आसान और सहज होता है।



हमेशा याद रखें, सिर्फ आधिकारिक स्टोर्स से वेरिफाइड ऐप्स ही डाउनलोड करें ताकि खतरनाक सॉफ्टवेयर से बचा जा सके। अपने ऐप लॉक के लिए मजबूत PIN का इस्तेमाल करें। अधिकतम सुरक्षा के लिए फोन पर डबल और ट्रिपल लॉक लगाएं।

## गतिविधि

### अपनी याददाश्त का टेस्ट करें

- (I) पासवर्ड मैनेजर का मुख्य काम क्या होता है?
- आपके सभी पासवर्ड्स को सुरक्षित तरीके से स्टोर और व्यवस्थित करना।
  - 5 मिनट तक कुछ ना करने पर ऑटोमैटिक लॉगआउट करना।
  - नए अकाउंट्स के लिए यूजरनेम बनाना।
  - ऐसे अकाउंट्स को डिलीट करना, जिन्हें आप अब इस्तेमाल नहीं करते।
- (II) इन पासवर्ड्स में से कौन सा दिखने में मजबूत लग सकता है, लेकिन सबसे कम सुरक्षित है?
- Password@123!
  - xT#4jG!@oLmN\$z
  - MySecureP@ss2024!
  - E!3xy&7#M@n2023
- (III) इनमें से कौन सलाह एक मजबूत पासवर्ड बनाने के लिए नहीं दी जाती?
- पासवर्ड कम से कम 8-12 अक्षरों का होना चाहिए।
  - पासवर्ड में आपका पूरा नाम या जन्म वर्ष होना चाहिए।
  - पासवर्ड में बड़े और छोटे अक्षर, नंबर और स्पेशल कैरेक्टर्स होने चाहिए।
  - पासवर्ड में "123456" जैसे आसान पैटर्न से बचना चाहिए।
- (IV) आपको टू-फैक्टर ऑथेंटिकेशन (2FA) क्यों ऑन करना चाहिए?
- लॉगिन करने की प्रक्रिया को तेज़ बनाने के लिए।
  - अपने अकाउंट की सुरक्षा को और मजबूत करने के लिए।
  - पासवर्ड को हर महीने ऑटोमैटिक अपडेट करने के लिए।
  - ताकि कोई भी आसानी से आपके अकाउंट तक पहुंच सके।

### जवाब की कुंजी:

- अपने सभी पासवर्ड को सुरक्षित और व्यवस्थित तरीके से रखना।
- (I) a) आपके सभी पासवर्ड्स को सुरक्षित तरीके से स्टोर और व्यवस्थित करना।
- (II) a) Password@123! (कारण: इसमें एक सामान्य शब्द, "password" और अनुमानित पैटर्न का उपयोग किया गया है, जिससे यह हैकिंग के लिए कमजोर हो जाता है।)
- (III) b) पासवर्ड में आपका पूरा नाम या जन्म वर्ष होना चाहिए। (कारण: व्यक्तिगत जानकारी के कारण पासवर्ड का अनुमान लगाना सरल हो जाता है।)
- (IV) b) अपने अकाउंट की सुरक्षा को और मजबूत करने के लिए।

## सुरक्षा खतरों को जानना

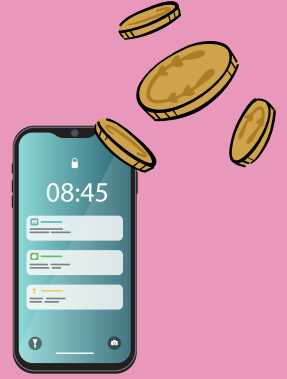


दोपहर की धूप बहुत अच्छी थी और रहीम पड़ोस के पार्क में बैठा हुआ था। कुछ बोर्ड गेम खेलने के बाद अब उसे एक नई चुनौती की तलाश थी! वह अपने दोस्त जसप्रीत और अमित भैया को पास में बैठे देखता है और उनके पास जाकर बैठ जाता है। जसप्रीत और रहीम मिलकर अमित भैया का फोन खोलते हैं और चुनौतीपूर्ण पहेलियों वाली कुछ नई वेबसाइटें खोजने लगते हैं।



अचानक, स्क्रीन पर ये संदेश दिखने लगता है!

बधाई हो! आपने गेम में 1,000 मुफ्त सिक्के जीत लिए हैं! अपना इनाम पाने के लिए यहाँ क्लिक करें और इस मैसेज का जवाब अपने फोन नंबर और OTP के साथ दें।

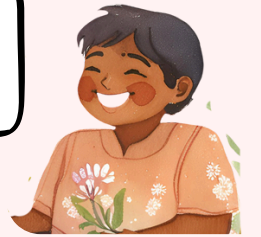


रहीम को इतने सारे सिक्के मिलने पर खुशी होती है, लेकिन वह इस बात को लेकर उलझन में रहता है कि उसे मैसेज पर क्लिक करना चाहिए या नहीं। जसप्रीत को भी मैसेज पर शक होता है और वे दोनों मिलकर इसे न खोलने का फैसला करते हैं।

यह मैसेज किसी आधिकारिक स्रोत से नहीं आया है और यह हमसे व्यक्तिगत जानकारी मांग रहा है – मुझे लगता है यह एक स्कैम हो सकता है! स्कैमर्स हमेशा नए तरीके ढूँढते रहते हैं ताकि हमारे डेटा, पैसे या डिवाइस चुरा सकें। ऐसे मैसेज से सावधान रहना जरूरी है। क्यों न हम ऑनलाइन खतरों के बारे में अपनी समझ को दोबारा देखें ताकि सुरक्षित रह सकें?



अरे हाँ! मुझे यकीन नहीं होता कि मजबूत पासवर्ड और सुरक्षा उपायों के बावजूद भी मुझे नुकसान पहुंचाया जा सकता है! मैं पूरी तरह से जागरूक रहना चाहता हूँ ताकि मैं अपनी और दूसरों की भी मदद कर सकूँ।



तो चलो हैकिंग से शुरुआत करते हैं! हैकर्स हमारे डेटा, जैसे कि पासवर्ड या बैंक की जानकारी, को देखने की कोशिश करते हैं और हमें बताए बिना उसे चुराने के तरीके खोजते हैं।

हाँ, पिछले साल मेरे कज़िन का अकाउंट हैक हो गया था! तब से मेरे परिवार के सभी लोग कई पासवर्ड और लॉक का इस्तेमाल कर रहे हैं।

## हैकिंग

हैकिंग का मतलब है बिना अनुमति के किसी के फोन, कंप्यूटर या ऑनलाइन अकाउंट में घुस जाना! हैकर्स पासवर्ड और सुरक्षा को बायपास करने के लिए कई कोड्स का इस्तेमाल करते हैं ताकि जानकारी चुराई जा सके या नुकसान पहुंचाया जा सके। हैकर्स निजी जानकारी चुरा सकते हैं, नुकसान कर सकते हैं या डिवाइस पर नियंत्रण भी ले सकते हैं। कुछ हैकर्स अवैध कारणों से ऐसा करते हैं, जबकि अन्य (जिन्हें "नैतिक हैकर्स" कहा जाता है) सुरक्षा की कमजोरियों को खोजने और उन्हें सुधारने का काम करते हैं। हैकर्स अक्सर डिवाइस को हैक करने के लिए मैलवेयर (एक कंप्यूटर सॉफ्टवेयर या वायरस जो गुप्त रूप से कंप्यूटर या नेटवर्क को नुकसान पहुंचाता है) का सहारा लेते हैं!



कल्पना करें कि आपके दोस्त की डायरी पर एक खास लॉक है, और जब वे इसे खोलती है, तो आप ध्यान से देखकर उसका पासवर्ड जान लेते हैं। आप चुपके से उनके निजी विचारों को पढ़ने के लिए उस पासवर्ड का इस्तेमाल करते हैं। यह हैकिंग की तरह है, लेकिन डायरी के बजाय, यह कंप्यूटर, फोन या खातों के साथ होता है!



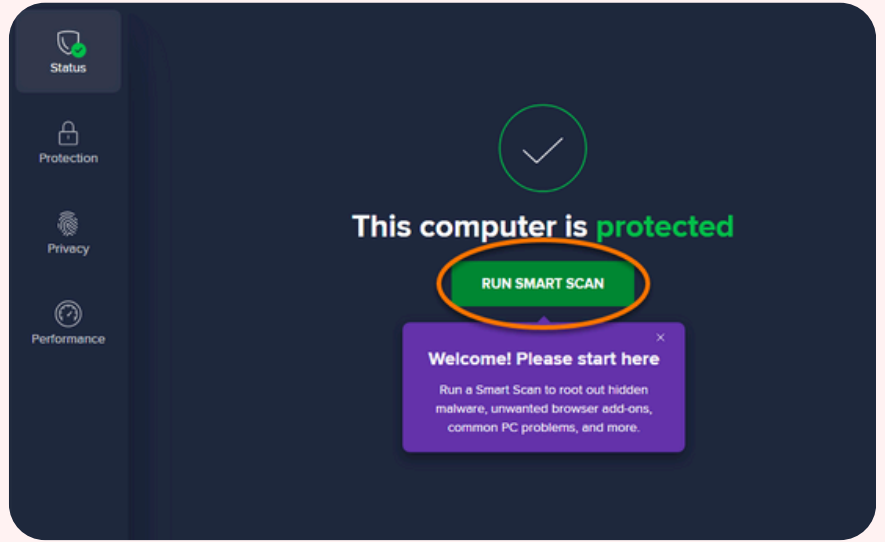
**टिप: एंटीवायरस सॉफ्टवेयर का इस्तेमाल करें और अपने डिवाइस को अपडेट रखें।**



एंटीवायरस सॉफ्टवेयर आपके कंप्यूटर से वायरस और दूसरे हानिकारक सॉफ्टवेयर को पहचानने और हटाने के लिए बनाया गया है। एंटीवायरस सॉफ्टवेयर इंस्टॉल करें, यह सुनिश्चित करें कि आपके डिवाइस का फ़ायरवॉल ऑन है, और बग या सुरक्षा छिद्रों को ठीक करने के लिए अपने डिवाइस को नियमित रूप से अपडेट करते रहें, क्योंकि हैकर्स इन्हीं का इस्तेमाल कर सकते हैं।

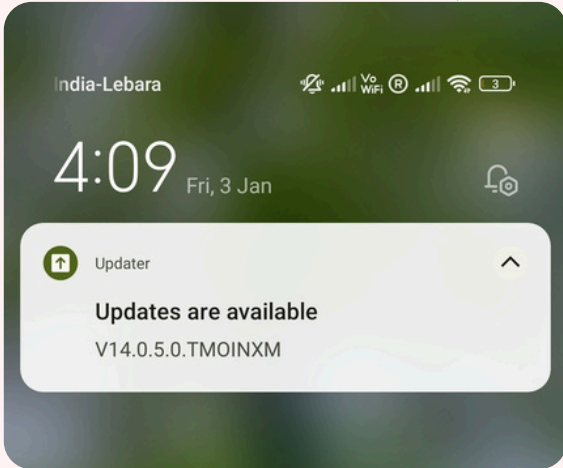
1

यह तस्वीर आपको यह दिखाती है कि एक भरोसेमंद एंटीवायरस सॉफ्टवेयर को कैसे डाला और चलाया जाता है। आपके पास चुनने के लिए कई सॉफ्टवेयर हैं, और किसी वयस्क से सलाह लेना या एक साधारण वेब खोज करना आपके निर्णय में मदद कर सकता है!



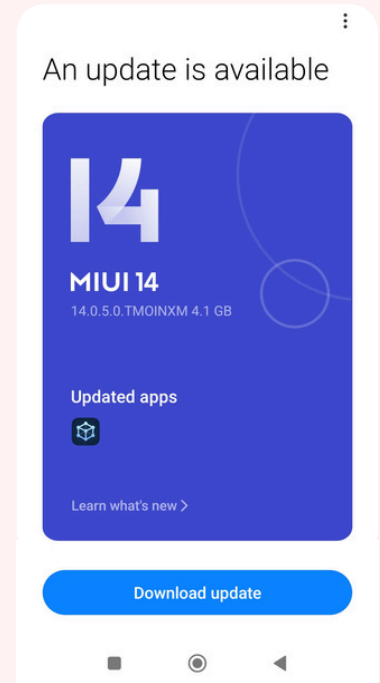
2

जब आपके फ़ोन में कोई अपडेट उपलब्ध होगा, तो यह आपको इस तरह की सूचना देगा:



3

नोटिफिकेशन पर क्लिक करने के बाद आप अपडेट डाउनलोड कर सकेंगे। हैकर्स से बचने के लिए आपको अपने फोन को नियमित रूप से अपडेट करना चाहिए!



## गतिविधि

आपने आखिरी बार अपने डिवाइस को कब अपडेट किया था? एक पल के लिए इस पर सोचें, और अगर आपने अभी तक अपडेट नहीं किया है, तो उसे अभी अपडेट कर लें!



क्या तुम्हें पता है कि एक और अलग तरह की हैकिंग होती है जिसमें कोई आपको धोखा देकर आपकी निजी जानकारी चुरा लेता है? इसे फ़िशिंग कहते हैं!

फ़िशिंग? मतलब तालाब में मछली पकड़ना, है ना?





खैर, कुछ हद तक! तुम इसे इस तरह समझ सकते हैं जैसे कोई व्यक्ति तुम्हारी जानकारी को छुपकर हासिल करने की कोशिश कर रहा है, कभी-कभी कोई और होने का बहाना बनाकर या तुम्हारे बैंक, स्कूल या पसंदीदा वीडियो गेम का नाम लेकर! हमें थोड़ी देर पहले जो मैसेज मिला, वह फ़िशिंग का एक बेहतरीन उदाहरण है!



## फ़िशिंग

फ़िशिंग एक चालाक तरीका है जिसमें धोखेबाज़ बिल्कुल असली लगने वाले नकली संदेश भेजते हैं! ये संदेश अक्सर हमें तुरंत कुछ करने के लिए उकसाते हैं, जैसे "अगर आप अभी वेरीफाई नहीं करते हैं, तो आपका खाता हटा दिया जाएगा!" ताकि हम घबरा जाएँ और लिंक पर क्लिक करें या पासवर्ड या क्रेडिट कार्ड नंबर जैसी संवेदनशील जानकारी भर दें। यह जानकारी फिर सीधे धोखेबाज़ के पास पहुँच जाती है। चलो फ़िशिंग का एक उदाहरण देखते हैं।

ध्यान दें: इस मैसेज में जल्दी जवाब देने का दबाव, नकली लिंक और व्यक्तिगत जानकारी मांगने जैसी बातें हैं – ये सभी खतरे की निशानियाँ हैं! हमेशा सतर्क रहें और किसी भी मैसेज या कॉल पर भरोसा न करें जो आपसे बैंकिंग जानकारी मांगता है।

9:00 PM

अमित भाईया



नया संदेश!

आपके खाते में 10,000 रुपये जमा हो चुके हैं! नीचे दिए गए लिंक पर क्लिक करें और अपना बैंक विवरण निःशुल्क भरकर अपना नकद पुरस्कार प्राप्त करें! यह एक बार का ऑफ़र है जो 30 मिनट में समाप्त हो जाएगा।

[www.W3kwithUS.co/account-login/index\\_4321xQz](http://www.W3kwithUS.co/account-login/index_4321xQz)



टिप: लिंक को जांचें!!

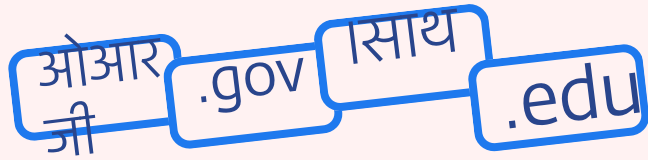


अगर आपको अचानक किसी अनजान स्रोत से लिंक मिले, जो अजीब लगे या किसी लुभावने ऑफ़र के साथ आए, तो उससे दूर रहें...कई बार, अजनबी लिंक आपकी जानकारी चुरा सकते हैं या आपके डिवाइस में खतरनाक वायरस डाउनलोड कर सकते हैं। हमेशा सतर्क रहें!

यहां कुछ सुझाव हैं जो आपको हानिकारक लिंक से बचने में मदद करेंगे और यह सुनिश्चित करेंगे कि आप एक सुरक्षित और भरोसेमंद वेबसाइट पर हैं।



- ब्राउज़र में जिस वेबसाइट का लिंक आप टाइप कर रहे हैं, उसे चेक करें, और यह सुनिश्चित करें कि वह "https" से शुरू हो रहा है। "S" का मतलब है सुरक्षित, और यह बताता है कि साइट डेटा की सुरक्षा के लिए एन्क्रिप्शन का इस्तेमाल कर रही है।



- सुनिश्चित करें कि लिंक का नाम ".com", ".org", ".gov", ".in" या ".edu.in" पर खत्म होता है - ये विश्वसनीय डोमेन नाम हैं।



- हमेशा वेबसाइट को ध्यान से जांचें - खासकर "About" सेक्शन को, ताकि पता चले किसने इसे बनाया है और इसका उद्देश्य क्या है।



- हमेशा URL को ध्यान से दोबारा जांचें ताकि यह सुनिश्चित हो कि यह किसी विश्वसनीय साइट की नकल या नकली वर्जन न हो। उदाहरण के लिए, "amaz0n.com" एक फर्जी साइट है जो असली "amazon.com" की नकल करने की कोशिश कर रही है।



- यह सुनिश्चित करने के लिए कि यह सही है और अन्य उपयोगकर्ताओं द्वारा विश्वसनीय माना जाता है, प्लेटफ़ॉर्म के बारे में ऑनलाइन रिव्यूज़ देखें।



जैसा कि नाम से ही समझ में आता है, एड ब्लॉकर्स इंटरनेट पर पॉप-अप, विज्ञापनों और अन्य अविश्वसनीय चीजों को ब्लॉक करते हैं, खासकर जब आप गलती से किसी पर क्लिक कर देते हैं। जैसे कि आप दाईं ओर देख सकते हैं, कुछ अविश्वसनीय वेबसाइटें आपसे आपके एड ब्लॉकर्स को बंद करने के लिए कह सकती हैं - जो कि असुरक्षित हो सकता है!

**Oops! An adblocker is enabled on your device**



Complete one of the following actions so that you don't lose your cashback:

- Add कैवरीशिय to [the list of exceptions](#)  
If it doesn't work, try to [do it manually](#) or choose one of the solutions below.
- Completely disable the adblocker. [How to do it.](#)

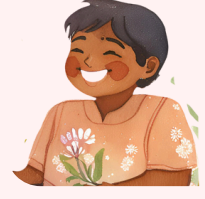
1 After this, it is necessary to [refresh the page.](#)

क्या आप एड ब्लॉकर का इस्तेमाल करते हैं? अपने ब्राउज़र में एक्सटेंशन के तौर पर एक भरोसेमंद एड ब्लॉकर इंस्टॉल करने की कोशिश करें!

फ़िशिंग वाकई में एक डरावनी चीज़ है! हैकर्स और "फ़िशर्स" इस सारी जानकारी का क्या करते हैं?



वे आपकी सारी जानकारी का उपयोग करके आपको ऑनलाइन धोखा दे सकते हैं। वे आपके नाम पर खाते खोल सकते हैं, आपके बैंक से पैसे निकाल सकते हैं और यहाँ तक कि आपके नाम पर लोन भी ले सकते हैं! इसे पहचान की चोरी कहते हैं।



## पहचान की चोरी



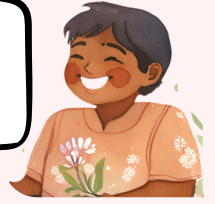
पहचान की चोरी तब होती है जब कोई व्यक्ति आपकी व्यक्तिगत जानकारी, जैसे कि नाम, पता या आधार कार्ड नंबर का इस्तेमाल करके आप होने का दिखावा करता है! वे ऐसा खाते खोलने, सामान खरीदने या कुछ गैरकानूनी काम करने के लिए कर सकते हैं, जबकि ऐसा लगता है कि यह आपकी गलती है। इससे आप बड़ी परेशानी में आ सकते हैं, जैसे कि उन चीज़ों के लिए दोषी ठहराया जाना जो आपने नहीं की हैं या अपने खुद के खातों तक पहुँच खोना। यहाँ कुछ उदाहरण दिए गए हैं!

मान लीजिए कि किसी को आपका खोया हुआ स्कूल आईडी कार्ड मिल जाता है और वह आपके रोल नंबर का इस्तेमाल करके आप बनके नकल करके आपका परीक्षा पेपर ले लेता है। शिक्षक उनकी बात पर विश्वास कर लेते हैं क्योंकि उन्हें लगता है कि यह सच में आप ही हैं - अब वे आपके परीक्षा स्कोर देख सकते हैं!



मान लीजिए कि किसी को किराने की दुकान पर खोया हुआ बटुआ मिल जाता है। उसे लौटाने के बजाय, वे उस व्यक्ति का नाम, उम्र और पता उसके पहचान पत्र से लेकर क्रेडिट कार्ड के लिए आवेदन कर देते हैं। फिर वे महंगी चीज़ें खरीदना शुरू कर देते हैं, और जब बिल आता है, तो वह बटुए के असली मालिक को भेज दिया जाता है, भले ही उन्होंने कभी उस पैसे को खर्च न किया हो!

तो मान लीजिए कि कोई इन तरीकों का इस्तेमाल करके मेरी पहचान, जानकारी और डेटा चुराने में सफल हो जाता है... तो वे इसके साथ और क्या कर सकते हैं?



दुर्भाग्य से, वे आपका डेटा बेच सकते हैं, उसका गलत इस्तेमाल कर सकते हैं और यहां तक कि इसका उपयोग कुछ लोगों को निशाना बनाने के लिए भी कर सकते हैं! इसे ही डेटा की चोरी कहते हैं।

## डेटा की चोरी

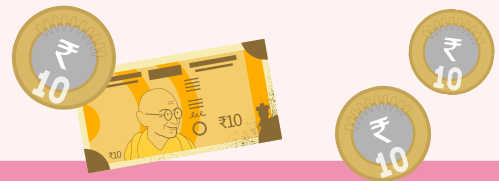
डेटा चोरी में बिना इजाजत के डिजिटल जानकारी, जैसे कि पासवर्ड, बैंक की जानकारी या मेडिकल रिकॉर्ड चुराना शामिल होता है। इस डेटा को बेचा जा सकता है या फिर आगे के अपराधों के लिए इस्तेमाल किया जा सकता है! अक्सर व्यवसायों को निशाना बनाया जाता है क्योंकि वे बड़ी मात्रा में ग्राहक जानकारी रखते हैं, लेकिन आम व्यक्ति भी शिकार बन सकते हैं।



मुझे लगता है कि अब मैं पहेली के सारे टुकड़ों को एक साथ जोड़ने लगा हूँ! लेकिन मुझे अभी भी यह समझ नहीं आ रहा है कि कोई ऐसा सब क्यों चुराएगा?



चलो अमित भैया से पूछते हैं! वो हमें और भी कुछ बता सकते हैं।



अरे वाह तुम दोनों वाकई में बहुत समझदार हो! हैकिंग, फ़िशिंग और डेटा और पहचान की चोरी जैसे सभी खतरों को गंभीरता से लेना जरूरी है, क्योंकि इनका इस्तेमाल अक्सर पैसों की धोखाधड़ी के लिए किया जाता है। यह तब होता है जब कोई आपके पैसे या वित्तीय जानकारी को चुरा लेता है। धोखाधड़ी ऑनलाइन या ऑफ़लाइन भी हो सकती है और इसे ठीक करना अक्सर मुश्किल होता है। इसलिए हमें बहुत सतर्क रहना चाहिए। यहाँ एक पैसों की धोखाधड़ी का उदाहरण है जो आपको खुद को बेहतर तरीके से सुरक्षित रखने में मदद करेगा - यह पिछले हफ्ते मेरी बहन के साथ हुआ था!

नमस्ते मैडम। मैं सुरेश, जिला बिजली बोर्ड से बोल रहा हूँ। यह एक बहुत जरूरी कॉल है। हमारे रिकॉर्ड के मुताबिक, आपका पिछला बिजली बिल नहीं भरा है, और अगले 2 घंटों में आपका कनेक्शन कटने का खतरा है।



क्या? मैंने तो पिछले हफ्ते ही अपना बिल चुका दिया था! जरूर कोई गलती हुई होगी।

मैं आपकी चिंता को समझता हूँ, मैडम, लेकिन हमें भुगतान की कोई पुष्टि नहीं मिली है। कनेक्शन कटने से बचने के लिए, मुझे आपसे ₹2,500 की बकाया राशि का तुरंत भुगतान करने की जरूरत है। चिंता मत कीजिए, मैं अभी फ़ोन पर आपको इसके बारे में बता सकता हूँ।



मुझे क्या करना चाहिए?

कृपया अपने फोन पर बैंकिंग ऐप खोलें, और मैं आपको भुगतान पूरा करने के लिए एक सुरक्षित लिंक दूंगा। किसी भी रुकावट से बचने के लिए सुनिश्चित करें कि आप इसे 5 मिनट के भीतर पूरा कर लें!



अमित की बहन उस लिंक पर क्लिक करती है, जो उसे एक फ़र्जी भुगतान पेज पर ले जाता है... और वह एक अनजान शख्स को फिर से अपना बिल चुका देती है!



क्या आपको इस बातचीत में कुछ संदिग्ध संकेत दिखे? यहाँ कुछ संकेत हैं जिन पर आप ध्यान दे सकते हैं:

#### जल्दी का दबाव और डर:

कॉल करने वाला व्यक्ति पीड़ित पर बिना सोचे-समझे कार्रवाई करने के लिए दबाव डालने के लिए घबराहट पैदा करता है।

#### असत्यापित पहचान:


कॉल करने वाला व्यक्ति खुद को किसी अधिकारी का प्रतिनिधि बताता है, लेकिन कोई सबूत नहीं पेश करता।

#### असामान्य भुगतान तरीका

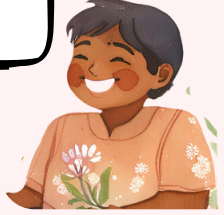
विश्वसनीय कंपनियां कभी-कभी ही व्यक्तिगत खातों या असुरक्षित लिंक के जरिए तुरंत भुगतान करने के लिए कहती हैं।

#### फ़र्जी लिंक:


कॉल करने वाले ने आधिकारिक भुगतान पृष्ठ के रूप में एक खतरनाक लिंक भेजा।




मेरी बहन ने बाद में देखा कि भुगतान वेबसाइट का लेआउट और URL गलत था। आपको क्या लगता है, मेरी बहन को घोटालेबाज की जांच करने और खुद को बचाने के लिए और क्या करना चाहिए था?



हम्म... वह फोन करने वाले से उसकी आईडी पूछ सकती थी और फिर बिजली कंपनी को फोन करके इसकी पुष्टि कर सकती थी? मुझे लगता है कि उसे नंबर भी ब्लॉक कर देना चाहिए था!



हम्म... उसे शायद अपने बैंक से भी चेक कर लेना चाहिए कि कुछ भी निकाला गया है या नहीं!



बहुत बढ़िया!! ये सारे सुझाव और सुरक्षा उपाय आपके लिए ऑनलाइन शॉपिंग करते समय भी फायदेमंद रहेंगे!



## आपकी ऑनलाइन शॉपिंग के लिए सुरक्षा चेकलिस्ट

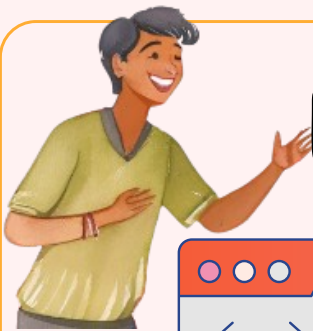
- रिव्यूस पढ़ें और जानें कि दूसरे ग्राहक उस चीज़ के बारे में क्या सोचते हैं। नकली रिव्यु या संदिग्ध सामग्री से सतर्क रहें।
- सुनिश्चित करें कि साइट सुरक्षित है, उसमें 'https://' है और एड्रेस बार में लॉक का आइकन है।
- उत्पाद का आकार, रंग और किसी भी खास विशेषता को अच्छी तरह से जांचें और सुनिश्चित करें कि यह बिल्कुल वही है जिसकी आपको ज़रूरत है। सिर्फ़ तस्वीरों पर भरोसा मत करें!
- क्या वेबसाइट ने आपसे पासवर्ड या बैंक की जानकारी मांगी? असली शॉपिंग साइट्स कभी भी कॉल, ईमेल या मैसेज के जरिए ऐसा नहीं पूछतीं!
- सुनिश्चित करें कि भुगतान गेटवे सुरक्षित है और संदिग्ध वेबसाइटों के साथ ओटीपी, कार्ड की जानकारी और सीवीवी कोड जैसी जानकारियाँ साझा करने से बचें।
- सुनिश्चित करें कि ऑर्डर के बारे में जो मैसेज हैं, वे असली हैं - इनमें आमतौर पर ऐसी चीज़ें नहीं होनी चाहिए: आपके द्वारा नहीं दिए गए ऑर्डर, लॉटरी, संवेदनशील जानकारी या मात्रा एवं लिखाई की गलतियाँ!
- अगर कोई उत्पाद आपकी उम्मीदों पर खरा नहीं उतरता है, तो प्रक्रिया को समझने के लिए नियम और शर्तें और धनवापसी नीति ज़रूर पढ़ें।

## क्या आपको पता है?

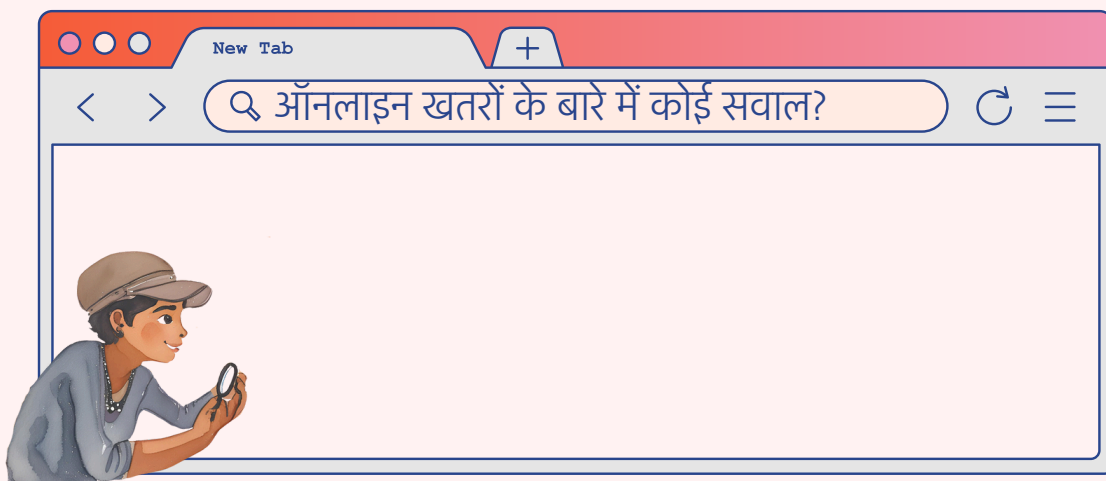
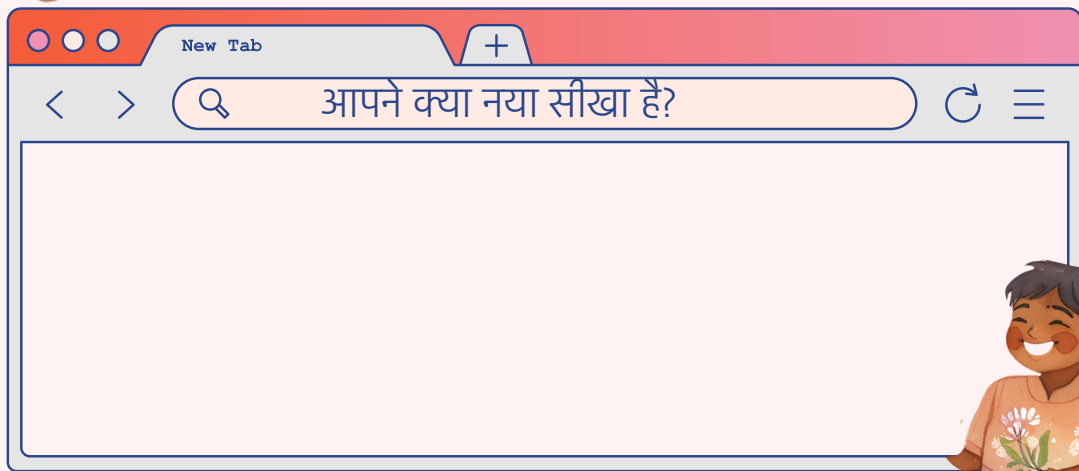
Amazon पर आप फ़िशिंग हमलों, संदिग्ध कॉल/ईमेल/टेक्स्ट या असुरक्षित/संदिग्ध चीज़ों के खिलाफ़ शिकायत कर सकते हैं। Amazon की सहायता सेवा के तहत...

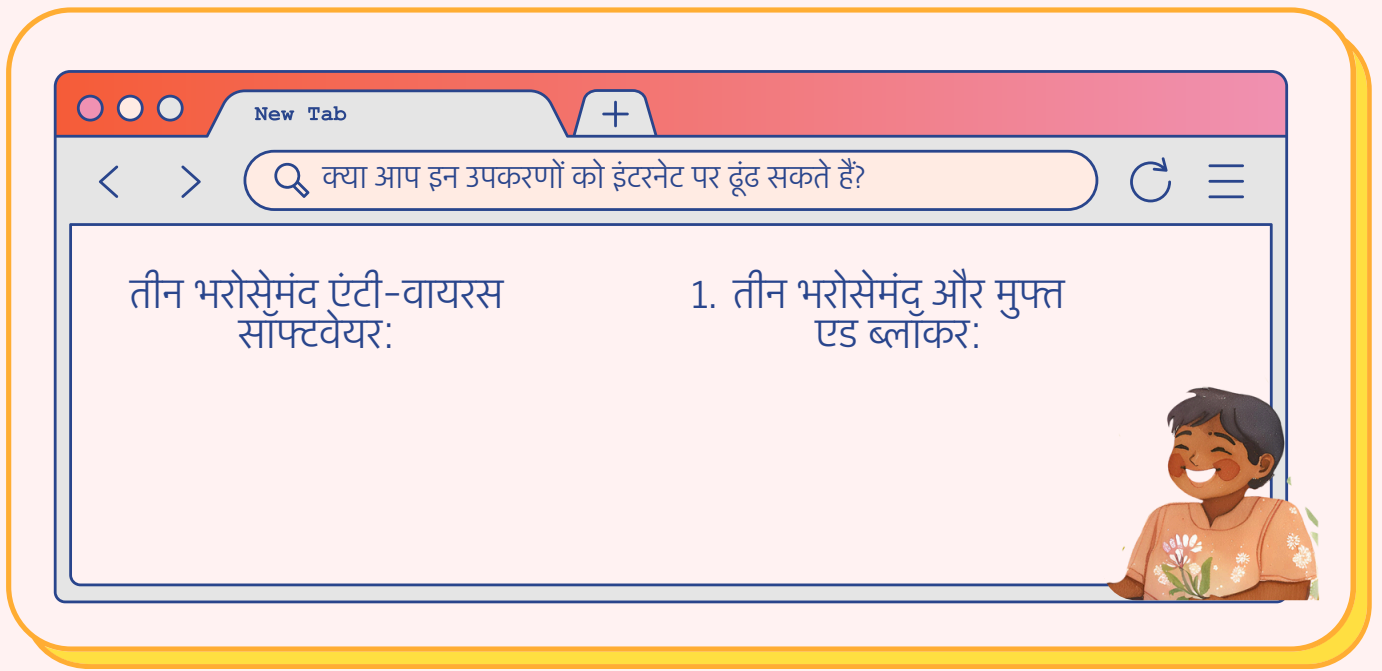
- ☆ "कुछ संदेहास्पद चीज़ की रिपोर्ट करना" पर जाएं और विकल्पों में से चयन करें। रिपोर्ट सबमिट करें और जरूरी जानकारी दें। संदिग्ध ईमेल/टेक्स्ट को reportascam@amazon.in पर फॉरवर्ड करें।
- ☆ संदिग्ध पैकेजेस की रिपोर्ट "अनचाहा पैकेज मिला" के तहत करें, बॉक्स को ध्यान से चेक करके जानकारी सबमिट करें।
- ☆ विक्रेताओं या प्रोडक्ट्स की रिपोर्ट सीधे प्रोडक्ट पेज से करें, "इस प्रोडक्ट या विक्रेता के साथ समस्या रिपोर्ट करें" पर क्लिक करें और निर्देशों का पालन करें।
- ☆ अमेज़न ने जो कुछ सामान्य घोटाले पहचाने हैं, वो यहां दिए गए हैं।

## गतिविधि



हमारे पास आपके लिए कुछ सवाल हैं!





## याद रखें: अपनी सुरक्षा के लिए ध्यान में रखने वाली बातें!

याद रखें, अगर आपको कुछ संदिग्ध लगे तो आपको अपने माता-पिता, शिक्षक या किसी और विश्वसनीय वयस्क से बात करनी चाहिए!



### मजबूत पासवर्ड

ऐसे पासवर्ड बनाएं जिन्हें अनुमान लगाना मुश्किल हो और जिनमें अक्षरों, संख्याओं और विशेष वर्णों का मिश्रण हो। अपने नाम, पालतू जानवर के नाम या "12345" जैसे सरल पासवर्ड का उपयोग करने से बचें। यदि आप साझा किए गए डिवाइस का उपयोग कर रहे हैं, तो प्रत्येक सत्र के बाद हमेशा लॉग आउट करना न भूलें।



### दोहरी सुरक्षा

अपने खातों पर अतिरिक्त सुरक्षा के लिए 2 फैक्टर ऑथेंटिकेशन का उपयोग करें। यह सुनिश्चित करता है कि यदि कोई आपका पासवर्ड जान भी ले, तो उसे लॉग इन करने के लिए दूसरा कोड भी चाहिए होगा। किसी भी खाते की सेटिंग्स में जाकर इसे गोपनीयता और सुरक्षा विकल्प के तहत ढूंढ सकते हैं।



### क्लिक करने से पहले थोड़ा सोचें!

ईमेल या संदेशों में दिए गए लिंक पर तब तक क्लिक न करें जब तक आप सुनिश्चित न हों कि वे सुरक्षित हैं। यदि कोई चीज़ संदिग्ध लगती है, तो सीधे कंपनी या व्यक्ति से संपर्क करके उसकी पुष्टि करें। साथ ही, ईमेल में वर्तनी की गलतियों, अजनबियों से आए संदेशों या पैसों के लिए की जा रही जल्दबाजी वाली मांगों पर विशेष ध्यान दें।

## याद रखें: अपनी सुरक्षा के लिए ध्यान में रखने वाली बातें!



### एडब्लॉकर्स

एड ब्लॉकर ऐसे सॉफ्टवेयर या ब्राउज़र एक्सटेंशन होते हैं जो वेबसाइटों पर आने वाले विज्ञापनों, जैसे पॉप-अप, बैनर और वीडियो ऐड्स को रोकते हैं। इससे इंटरनेट तेज चलता है, कम डेटा खर्च होता है और खतरनाक विज्ञापनों से बचाव होता है, जो वायरस फैला सकते हैं।



### सार्वजनिक वाई-फाई से दूर रहें और ब्लूटूथ को बंद कर दें।

सार्वजनिक वाई-फाई का उपयोग करना या ब्लूटूथ चालू रखना आपके डेटा को खतरे में डाल सकता है। सुरक्षित रहने के लिए हमेशा निजी और सुरक्षित नेटवर्क का इस्तेमाल करें और जब जरूरत न हो तो ब्लूटूथ बंद रखें।



### ऑनलाइन क्या शेयर करना है, इस पर ध्यान दें।

सोशल मीडिया पर अपना पूरा नाम, पता, फ़ोन नंबर या स्कूल का नाम जैसी निजी जानकारी शेयर करने से बचें! सोशल मीडिया और गेम पर गोपनीयता सेटिंग्स का इस्तेमाल करके यह नियंत्रित करें कि आपकी प्रोफ़ाइल, पोस्ट और मैसेज कौन देख सकता है। जल्द ही, हम यह जानेंगे कि इसे कैसे किया जाए!



### एंटीवायरस सॉफ़्टवेयर का इस्तेमाल करें और अपने डिवाइस को अपडेट करें।

एंटीवायरस सॉफ़्टवेयर इंस्टॉल करें और यह सुनिश्चित करें कि आपके डिवाइस का फ़ायरवॉल चालू है। ये टूल्स हानिकारक मेलवेयर और वायरस को पहचानने और उन्हें ब्लॉक करने में मदद करते हैं, जिनका उपयोग हैकर आपकी जानकारी चुराने के लिए करते हैं। आपको बग या सुरक्षा छिद्रों को ठीक करने के लिए अपने डिवाइस को नियमित रूप से अपडेट करना चाहिए, जिससे हैकर्स अंदर घुसने की कोशिश कर सकते हैं।



### अपने डेटा का बैकअप जरूर लें।

महत्वपूर्ण फ़ाइलों या फ़ोटो की कॉपियाँ नियमित रूप से बाहरी हार्ड ड्राइव या क्लाउड सेवा पर सेव करें। अगर आपका डिवाइस कभी हैक हो जाता है या वायरस से संक्रमित हो जाता है, तो आप सब कुछ नहीं खोएंगे।



# चैप्टर 3: गोपनीयता: आपकी डिजिटल ढाल



मीरा, रहीम और सुज़ैन पार्क में धूप का मज़ा ले रहे हैं, हँसते-मज़ाक करते हुए सेल्फी ले रहे हैं। मीरा को उनकी एक तस्वीर बहुत प्यारी लगती है। वह उसे अपलोड करती है और लोकेशन टैग करते हुए उन्हें टैग करती है!



रुको, मीरा, तुमने मुझे टैग किया और लोकेशन भी जोड़ दी? मुझे यह पसंद नहीं है।

अरे! क्यों नहीं? यह तो बस एक मजेदार फोटो है। लोकेशन टैग करने में क्या बुराई है?



मुझे अजीब लगता है। असली टाइम में अपनी लोकेशन शेयर करना थोड़ा रिस्की होता है। पहले पूछ तो लेना चाहिए ना!



हर कोई ऐसे ही फोटोज़ पोस्ट करता है, रहीम। तुम बेकार में परेशान हो रहे हो, कुछ नहीं होने वाला।



बात ये नहीं है! मैं तुम्हें ये कैसे समझाऊं उफ़फ़....



रहीम, क्यों न हम किसी ऐसे इंसान के पास चलें जो मीरा को इस बात को समझने में मदद कर सके? चलो अमित भैया से मिलते हैं!



अरे वाह, सब लोग आ गए! मुझे खुशी है कि तुम लोग मुझसे मिलने आए। अब तो तुम सब इंटरनेट के एक्टिव यूजर्स बन रहे हो। यही सही समय है ऑनलाइन गोपनीयता, सहमति, और सीमाओं के बारे में सीखने का! तो चलो, शुरू करते हैं!

## गोपनीयता, सहमति और सीमाओं को समझना

गोपनीयता का मतलब है आपके बारे में कौन क्या जानकारी जानता है यह खुद तय करना। अलग-अलग लोग गोपनीयता के अलग-अलग स्तर पसंद करते हैं - उदाहरण के लिए, कुछ लोग अपने जन्मदिन सबको बताना करना पसंद नहीं करते हैं, जबकि कुछ लोग नहीं! लेकिन जैसे हम ऑफलाइन अजनबियों से अपनी लोकेशन या पर्सनल बातें शेयर करने से बचते हैं, वैसे ही ऑनलाइन भी अपनी गोपनीयता बनाए रखना और बढ़ाना हमें सुरक्षित रखने में मदद करता है।

2017 में, भारत में एक महत्वपूर्ण मामला, जिसे पुट्टास्वामी जजमेंट के नाम से जाना जाता है, ने आधिकारिक रूप से प्राइवैसी (गोपनीयता) को हर नागरिक का मौलिक अधिकार माना। यह फैसला एक बड़ा बदलाव था, क्योंकि इसने यह साफ कर दिया कि हर व्यक्ति को अपने निजी स्पेस, जानकारी और चुनावों पर पूरा हक है। इसे ऐसे समझें: जैसे आप अपनी ऑनलाइन एक्टिविटी के बारे में अपने माता-पिता या दोस्तों से सबकुछ शेयर करना जरूरी नहीं समझते, यह पूरी तरह से आपका फैसला होता है। आपको तय करने का अधिकार है कि आप क्या शेयर करना चाहते हैं और किसके साथ। यही गोपनीयता का असली मतलब है—आपकी अपनी जानकारी और सीमाओं पर आपका कंट्रोल। इस अध्याय में, हम सीखेंगे कि डिजिटल दुनिया में अपनी प्राइवैसी को बेहतर तरीके से कैसे समझें और सुरक्षित रखें।

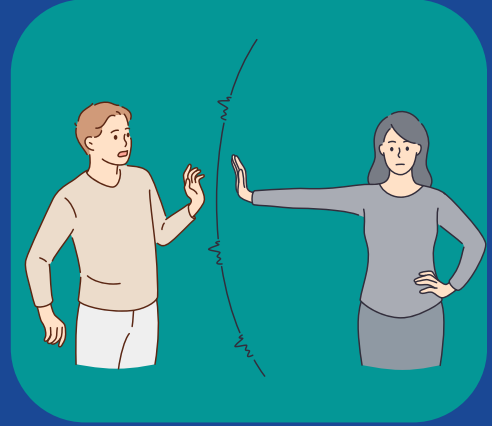


## डिजिटल सहमति क्या है?

डिजिटल सहमति का मतलब है कि आप अपनी निजी जानकारी, तस्वीरें या ऑनलाइन अनुभवों को किसी के साथ शेयर करने की साफ़ और स्पष्ट अनुमति दें। इसका मतलब यह भी है कि आप सोच-समझकर और जानकारी लेकर तय करें कि आपको क्या शेयर करने में सहज महसूस होता है। यह फ़ोटो, मैसेज या आपकी लोकेशन जैसी चीज़ों पर भी लागू होता है। सबसे जरूरी बात - डिजिटल सहमति को कभी भी बदला जा सकता है! अगर आपने पहले हां कहा था लेकिन बाद में असहज महसूस करने लगे, तो आप मना कर सकते हैं। यह समझना बहुत जरूरी है कि सहमति ज़बरदस्ती नहीं ली जा सकती, न ही इसे अपने आप मान लिया जा सकता है। सहमति हमेशा खुलकर और खुशी से दी जानी चाहिए।

## सीमाएँ: सहमति का एक पैटर्न

सीमाएँ वे अदृश्य रेखाएँ होती हैं जो यह तय करती हैं कि आप खुद को सुरक्षित और सहज कैसे महसूस करते हैं। डिजिटल दुनिया में, ये सीमाएँ आपको यह तय करने में मदद करती हैं कि क्या शेयर करना है, किस पर भरोसा करना है, और दूसरों से क्या उम्मीद रखनी है। एक बार जब आप अपनी सीमाएँ तय कर लेते हैं, तो आप उनके आधार पर सहमति देने या इनकार करने का फैसला कर सकते हैं। उदाहरण के लिए, अगर आपको यह पसंद है कि कोई आपकी फ़ोटो पोस्ट करने से पहले आपसे पूछे या आप अपनी लोकेशन सिर्फ़ करीबी दोस्तों के साथ ही शेयर करना चाहते हैं, तो ये सीमाएँ आपके फैसले तय करने में मदद करेंगी। इससे न केवल आप खुद को सुरक्षित रख सकते हैं, बल्कि दूसरे लोग भी आपकी पसंद और सहूलियत का सम्मान करेंगे।



## गोपनीयता बनाम सुरक्षा

गोपनीयता आपकी व्यक्तिगत जानकारी पर नियंत्रण के बारे में है, जबकि सुरक्षा आपके डेटा और डिवाइस को बाहरी खतरों से बचाने के बारे में है। वे आपस में जुड़े हुए हैं - मजबूत सुरक्षा अक्सर गोपनीयता के साथ होती है, और गोपनीयता का ध्यान रखना बेहतर सुरक्षा बनाए रखने में मदद करता है।

## गतिविधि

पहचान करें कि निम्नलिखित कार्य गोपनीयता, सुरक्षा या दोनों के लिए उपाय हैं:

- प्रत्येक खाते के लिए मजबूत, और अलग पासवर्ड बनाना।
- काम उपयोग किये जाने वाले ऐप्स के लिए लोकेशन शेयर बंद करना।
- उपयोग के बाद शेयर्ड डिवाइसों पर अपने खातों से लॉग आउट करना।
- अपने सोशल मीडिया अकाउंट को निजी रखना।
- अपना सोशल मीडिया यूजर नाम शेयर ना करना।

## गतिविधि

### व्यक्तिगत गोपनीयता और सीमाओं पर विचार करना

बिंगो कार्ड पर हर एक कथन को देखें और उन पर निशान लगाएं जिन बातों से आप ऑनलाइन सहज महसूस करते हैं।

यदि आप कोई पंक्ति, स्तंभ या विकर्ण पूरा कर लेते हैं, तो चिल्लाएं "बिंगो!"

मुझे अपना जन्मदिन ऑनलाइन शेयर करने में सहज महसूस होता है।	मैं सोशल मीडिया पर एक निजी अकाउंट का उपयोग करता/करती हूँ।	मैं पोस्ट में अपनी असली लोकेशन शेयर करने से बचता/बचती हूँ।	मुझे अपना ईमेल पता ऑनलाइन शेयर करना पसंद नहीं है।
मुझे असहज महसूस होता है जब कोई मुझसे बिना पूछे मुझे टैग कर देता है।	मुझे तस्वीरें शेयर करने में कोई दिक्कत नहीं है, लेकिन केवल करीबी दोस्तों के साथ।	मैं अपना फोन नंबर ऑनलाइन शेयर नहीं करना चाहता/चाहती।	मुझे असहज महसूस होता है जब कोई दोस्त बिना पूछे स्टोरी पर मेरी फोटो शेयर कर देता है।
मैं हमेशा शेयर करने से पहले यह सोचता/सोचती हूँ कि मेरी पोस्ट कौन देख सकता है।	मैं अपने स्कूल या घर का पता जैसी व्यक्तिगत जानकारी पोस्ट करने से बचता/बचती हूँ।	मैं किसी से भी मेरे बारे में पोस्ट हटाने के लिए कहने में सहज महसूस करता/करती हूँ।	मैं सोशल मीडिया पर कोई भी निजी बात शेयर करने से पहले दो बार सोचता/सोचती हूँ।
मैं अपने बारे में केवल अच्छी अपडेट साझा करना पसंद करता/करती हूँ।	मुझे ऑनलाइन चर्चाओं में अपने विचार शेयर करने में कोई दिक्कत नहीं है।	मुझे कोई दिक्कत नहीं अगर कोई मेरे साथ ग्रुप फोटो शेयर करता है।	मैं अजनबियों से फ्रेंड रिक्वेस्ट स्वीकार नहीं करता/करती।

क्या इन में से किसी वाक्य ने आपको रुकने या अधिक गहराई से सोचने पर मजबूर किया?

क्या आपने इस बात पर गौर किया कि आप किस चीज के साथ सहज हैं?

क्या इस गतिविधि के आधार पर आप अपने लिए कोई नई सीमाएँ तय करना चाहेंगे?

अब तुम्हें समझ में आया कि रहीम क्या कहना चाह रहा था, मीरा?



हाँ, मुझे समझ आ गया! और मुझे पहली बार न समझने के लिए बहुत बुरा लग रहा है। माफ़ करना, रहीम! मुझे फोटो में तुम्हें टैग करने से पहले तुमसे इजाजत लेनी चाहिए थी।



कोई बात नहीं! मुझे खुशी है कि हमने अमित भैया से बात की। वैसे भी, मुझे नहीं लगता कि मैंने तुम्हें ठीक से समझा पाया था।



मुझे भी कभी अपने दोस्तों और परिवार को समझाने के लिए सही शब्द नहीं मिलते। अमित भैया, क्या आप हमें यह सिखा सकते हैं कि हम अपनी ऑनलाइन सीमाएँ दूसरों को कैसे समझाएँ, बिना उनसे झगड़े किए या उन्हें दुखी किए?



मैं समझ गया, दोस्तो! अगली बार जब तुम्हें ऐसी कोई बातचीत करनी पड़े, तो बस इन बातों को याद रखें

- **आपकी टोन मायने रखती है:** इस तरह से बोलें जिससे लगे कि आप नाराज़ या परेशान नहीं हैं। आप चिल्लाने या नाराज़ होने के बजाय बस इतना कह सकते हैं कि "मैं बस यह बताना चाहता हूँ कि मैं इस बारे में कैसा महसूस करता/करती हूँ।"
- **भावनात्मक शब्दों का प्रयोग करें:** सीमाएँ क्यों ज़रूरी हैं, यह समझाने के लिए अपनी भावनाओं को व्यक्त करें। उदाहरण के लिए, "ऐसा मत करो" कहने के बजाय कहें "मुझे अपनी सुरक्षा की चिंता महसूस होती है।"
- **सुनें और सवालों के लिए तैयार रहें:** अपनी सीमाएँ बताने के बाद, दूसरे व्यक्ति को सवाल पूछने या अपने विचार पेश करने दें। हमें सिर्फ नियम नहीं बताने हैं बल्कि सामने वाले व्यक्ति से बातचीत करनी है। इसी तरह हम सब सीखते हैं!

मीरा और रहीम, चलो अब इन सब को ध्यान में रख कर ये बात करने की कोशिश करो, ठीक है?

ज़रूर!

मीरा, अपनी लोकेशन ऑनलाइन शेयर करने से मुझे चिंता होती है, और मैं उन पोस्ट्स में टैग होने में सहज महसूस नहीं करता जो तुम्हारी फ्रेंड लिस्ट को दिखाती हैं, क्योंकि मैं तुम्हारे सभी दोस्तों को नहीं जानता। क्या तुम टैग और लोकेशन हटा सकती हो?



ओह... मैंने इस बारे में सोचा ही नहीं। मुझे लगा कि ये ठीक होगा। माफ़ करना, रहीम। मेरा इरादा तुम्हें असहज करने का नहीं था। मैं अभी पोस्ट से टैग और लोकेशन हटा देती हूँ।

वाह, यह तो आसान था!  
धन्यवाद, भैया!

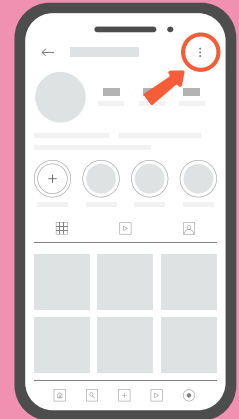


## गोपनीयता सेटिंग बढ़ाना

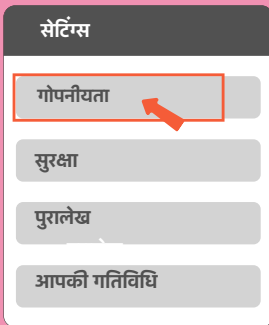
अब जब हमने अपनी निजी सीमाएँ तय कर ली हैं, तो आइए देखें कि अलग-अलग प्लेटफॉर्म पर अपनी गोपनीयता कैसे सुरक्षित रखें। इसमें यह समझना जरूरी है कि सोशल मीडिया, ईमेल अकाउंट और ऐप्स आपकी व्यक्तिगत जानकारी को कैसे संभालते हैं। यह जानना कि वे कौन-कौन सा डेटा इकट्ठा करते हैं और उसका इस्तेमाल कैसे करते हैं, आपको अपने ऑनलाइन मौजूदगी पर नियंत्रण रखने में मदद करेगा।



यहाँ रुकें और जाँचें कि आपका सोशल मीडिया अकाउंट पब्लिक है या प्राइवेट। अगर आपको नहीं पता कि कैसे जाँचें, तो इन चरणों का पालन करें अपना सोशल मीडिया ऐप खोलें और अपनी प्रोफाइल सेटिंग पर जाएं।



2. गोपनीयता सेटिंग या खाता सेटिंग जैसे विकल्प देखें।

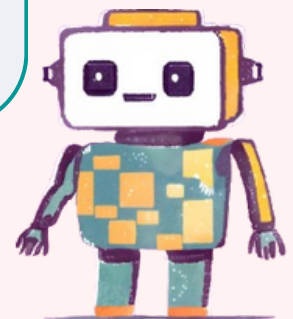


3. यदि आपका खाता सार्वजनिक है, तो आप इसे निजी बना सकते हैं ताकि आपकी प्रोफाइल केवल चुने हुए लोग ही देख सकें।

निजी खाते



याद है, हमने पहले चैप्टर में डिजिटल फुटप्रिंट के बारे में बात की थी? यह वही निशान होता है जो आप हर बार ऑनलाइन जाने पर छोड़ते हैं। ऐप्स, वेबसाइटें और सोशल मीडिया प्लेटफॉर्म अक्सर इस डेटा को इकट्ठा करते हैं ताकि वे आपकी पसंद के अनुसार चीजें दिखा सकें—जैसे टारगेटेड विज्ञापन, वीडियो सिफारिशें, या आपकी पसंद को पहले से समझना। यह सुविधाजनक लग सकता है, लेकिन यह जानना जरूरी है कि आप कितना डेटा शेयर कर रहे हैं और इसे कैसे नियंत्रित कर सकते हैं।



## कैश और कुकीज़: वे क्या हैं?

जब आप किसी वेबसाइट पर जाते हैं, तो वह कभी-कभी आपकी गतिविधि को "याद" रखती है। ऐसा कैश और कुकीज़ की वजह से होता है:

- कैश: इसे अपने ब्राउज़र का बैकपैक समझें, जो वेबसाइटों के कुछ हिस्सों (जैसे फोटोज़ और स्क्रिप्ट) को जमा करता है, ताकि अगली बार जब आप वेबसाइट पर जाएं तो वे तेज़ी से लोड हों।
- कुकीज़: ये वेबसाइट द्वारा जमा की गई जानकारी के छोटे-छोटे टुकड़े होते हैं, जैसे आपने किस पर क्लिक किया, अपने कार्ट में क्या जोड़ा, या यहां तक कि आपने किसी पेज पर कितना समय बिताया।

कुकीज़ वेबसाइटों को आपकी गतिविधि को ट्रैक करने की अनुमति देती हैं, जबकि कैश का उपयोग आपके डिवाइस तक पहुंचने वाले किसी व्यक्ति द्वारा यह देखने के लिए किया जा सकता है कि आप ऑनलाइन कहाँ कहाँ गए। यह ऐसा महसूस हो सकता है जैसे कि ब्राउज़ करते समय कोई आपके पीछे से झाँक रहा हो।

## गोपनीयता नीतियाँ और उपकरण

जब आप किसी नए गेम या ऐप के लिए साइन अप करते हैं, तो अक्सर आपसे गोपनीयता पॉलिसी को मानने के लिए कहा जाता है। यह एक दस्तावेज़ होता है जो बताता है कि आपका डेटा कैसे इकट्ठा, स्टोर, शेयर या इस्तेमाल किया जाएगा। लेकिन ज्यादातर लोग इसे नहीं पढ़ते क्योंकि यह बहुत लंबा या समझने में मुश्किल होता है।

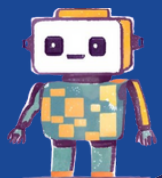
कुछ ऐप्स और वेबसाइटें आपके डेटा का सही इस्तेमाल करती हैं, लेकिन कुछ इसे दूसरों के साथ शेयर या बेच भी सकती हैं। गोपनीयता पॉलिसी को समझना जरूरी है ताकि आप सोच-समझकर फैसला ले सकें कि आप किससे सहमत हो रहे हैं। आप ऑनलाइन ऐसे टूल्स देख सकते हैं जो गोपनीयता पॉलिसी को आसान भाषा में समझाते हैं। इसके अलावा, कुछ टूल्स यह भी बताते हैं कि कोई वेबसाइट या ऐप आपके डेटा की सुरक्षा को कितना गंभीरता से लेती है।

## ऐप अनुमतियाँ

जब आप कोई नया ऐप डाउनलोड करते हैं, तो वह कैमरा, लोकेशन या कॉन्टैक्ट्स जैसी सुविधाओं की अनुमति मांग सकता है। कुछ अनुमतियाँ ऐप के सही तरीके से काम करने के लिए जरूरी होती हैं, लेकिन कुछ अनावश्यक हो सकती हैं और आपके डेटा के गलत इस्तेमाल का खतरा बढ़ा सकती हैं।

उदाहरण के लिए, एक फोटो एडिटिंग ऐप को आपकी लोकेशन की जरूरत नहीं होनी चाहिए। सुरक्षित रहने के लिए, ध्यान दें कि ऐप को कौन-सी अनुमति वास्तव में चाहिए, डिवाइस सेटिंग्स में जाकर गैर-जरूरी अनुमति बंद करें, और उन ऐप्स से बचें जो इंस्टॉल होते ही बहुत सारी अनुमतियाँ मांगते हैं।

हमने अभी देखा कि ऐप और वेबसाइट हमारी गोपनीयता को कैसे प्रभावित कर सकते हैं। अब, आइए इस बात पर ध्यान दें कि अन्य इंटरनेट उपयोगकर्ता इसे कैसे प्रभावित कर सकते हैं, साथ ही इन स्थितियों को पहचानने और उनका समाधान करने के तरीके के बारे में सुझाव भी दें।



## ऑनलाइन गोपनीयता उल्लंघन

मीरा, रहीम और सुसान अमित भैया और ग्लिच से मिलने के लिए उत्साहित हैं ताकि वे पार्क में बिताए गए अपने पिछले दिन के अनुभव साझा कर सकें। मीरा थोड़ा शर्मिंदा महसूस कर रही है, लेकिन वह अमित भैया को एक जरूरी सबक बताने के लिए उत्सुक है—ऑनलाइन कोई भी तस्वीर शेयर करने से पहले उसमें मौजूद लोगों की अनुमति लेना जरूरी है।



बहुत बढ़िया मीरा, यह वास्तव में एक बहुत ही जरूरी सीख है, लेकिन क्या तुम जानती हो कि बिना सहमति के तस्वीरों को साझा करना काफी आम बात है?

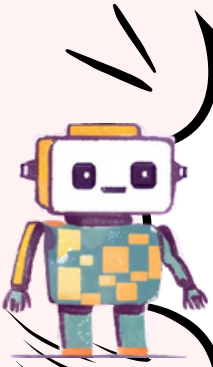
सच में? मुझे लगता है कि हम सभी को इस बारे में और बातचीत करनी चाहिए कि यह क्यों जरूरी है। क्या आप मुझे और बता सकते हैं?



बिना सहमति के तस्वीरें शेयर करना मतलब किसी की फोटो या वीडियो को बिना उनसे पूछे या उनके जाने किसी और को भेज देना। यह ग्रुप चैट, सोशल मीडिया या निजी संदेशों के ज़रिए भी हो सकता है। यह गोपनीयता का उल्लंघन है और इसके गंभीर परिणाम हो सकते हैं।

### बिना सहमति के साझा करना हानिकारक क्यों है?

- **यह गोपनीयता का उल्लंघन करता है:** बिना अनुमति किसी की तस्वीर शेयर करना उनके उस अधिकार का हनन करता है, जिससे वे तय कर सकें कि उनकी निजी जानकारी, जैसे तस्वीरें, कौन देख सकता है।
- **यह बुलीडिंग या उत्पीड़न का कारण बन सकता है:** बिना सोचे-समझे तस्वीरें शेयर करने से लोग बुरे कमेंट कर सकते हैं या तस्वीरों का गलत इस्तेमाल कर सकते हैं, जिससे भावनात्मक नुकसान हो सकता है।
- **यह किसी को चिंतित, असुरक्षित या शर्मिंदा महसूस करा सकता है:** बिना सहमति के तस्वीरें शेयर होने पर कोई व्यक्ति असहज, दुखी या असुरक्षित महसूस कर सकता है।



अगर किसी की सहमति को लेकर संदेह हो, तो बस पूछ लें! अंदाज़ा से बेहतर है कि पहले उनकी सीमाओं के बारे में जान लें।

क्या आप अपनी और दूसरों की ऑनलाइन गोपनीयता की सुरक्षा करना चाहते हैं? यह "सही या गलत" क्विज़ लें और देखें कि आप सही रास्ते पर हैं या नहीं!

-अगर कोई आपका दोस्त है, तो बिना पूछे उसकी फोटो शेयर करना ठीक है। (सही/गलत)

-अगर कोई बिना अनुमति किसी दोस्त की फोटो ग्रुप चैट में शेयर करके उसका मज़ाक उड़ाता है, तो इसे नजरअंदाज करना और चैट जारी रखना ठीक है। (सही/गलत)

-किसी ग्रुप फोटो तो बिना पूछे लोगों को टैग करना ठीक है। (सही/गलत)



आइए कुछ ऐसे तरीकों पर नज़र डालें जिनसे लोगों की ऑनलाइन गोपनीयता और सुरक्षा खतरे में आ सकती है। ये डरावने लग सकते हैं, लेकिन चिंता न करें, इन्हें पूरी तरह से समझ लेना सुरक्षित रहने का पहला कदम है।

## बुलिंग

आपने बुलिंग (धमकाने) के बारे में तो सुना ही होगा—अक्सर इसे शारीरिक रूप में समझा जाता है, जैसे किसी को धक्का देना या सामने से चिढ़ाना। लेकिन क्या आप जानते हैं कि बुलिंग ऑनलाइन भी होती है? यह उतनी ही नुकसानदायक हो सकती है, बल्कि कभी-कभी उससे भी ज्यादा, क्योंकि यह बड़ी संख्या में लोगों तक पहुंच सकती है और किसी भी समय, कहीं भी हो सकती है।



ऑनलाइन बुलिंग, जिसे 'साइबरबुलिंग' के नाम से भी जाना जाता है, कई अलग-अलग रूप लेती है। यह सिर्फ बुरे शब्दों के बारे में नहीं है; इसमें किसी की निजी जानकारी बिना अनुमति शेयर करना (डॉक्सिंग), चोट पहुंचाने वाले कमेंट पोस्ट करना (ट्रोलिंग) और किसी को ऑनलाइन ग्रुप्स से बाहर करना (एक्सक्लूशन) जैसी हरकतें शामिल हो सकती हैं।

### डॉक्सिंग

डॉक्सिंग तब होता है जब कोई आपकी व्यक्तिगत जानकारी, जैसे आपका पता या फोन नंबर, आपकी सहमति के बिना ऑनलाइन शेयर कर देता है।

### ट्रोलिंग

ट्रोलिंग तब होती है जब कोई व्यक्ति दूसरों को परेशान करने के लिए चोट पहुंचाने वाली या परेशान करने वाली टिप्पणियां पोस्ट करता है।

### एक्सक्लूशन

एक्सक्लूशन तब होता है जब किसी व्यक्ति को ऑनलाइन समूहों या चैट से जानबूझकर बाहर रखा जाता है ताकि उसे बुरा महसूस हो।



## दूसरों की जगह खुद को रखकर देखें : ट्रोलिंग को समझें

कल्पना कीजिए कि आप किसी से ऑनलाइन बातचीत कर रहे हैं और अचानक कोई आपको चोट पहुंचाने वाले शब्दों से निशाना बनाना शुरू कर देता है। यह सिर्फ "चिढ़ाना" नहीं है; यह ट्रोलिंग है - जानबूझकर और लगातार की जाने वाली हरकतें जिसका मकसद उकसाना या अपमानित करना है। आइए एक उदाहरण देखें:

प्रिय डायरी,

आज साइंस प्रोजेक्ट पर चर्चा कुछ ऐसी हो गई जिसकी मुझे उम्मीद नहीं थी। आर्यन ने लिखा, "समीर को कोई ज़रूरी काम मत देना। वह पिछली बार की तरह गड़बड़ कर देगा।" सब ने इस मैसेज को लाइक किया, मुझे बहुत अपमानित महसूस हुआ।

फिर कुणाल ने मेरे परिवार की कुछ पुरानी तस्वीरें पोस्ट कर दी। मुझे नहीं पता कि उसे यह कैसे मिली - मुझे ये मेरी प्राइवैसी का उल्लंघन लगा।

रिया ने कहा, "चलो समीर को इस प्रोजेक्ट से बाहर कर देते हैं। वह किसी काम का नहीं है।" और उन्होंने कहा, "हम इस बारे में पर्सनल ग्रुप में बात करेंगे, यहाँ समीर के साथ नहीं।" मुझे पूरी तरह से अलग-थलग महसूस हुआ।

आर्यन ने फिर पोस्ट किया, "समीर अपना हिस्सा भी पूरा नहीं करेगा। वह बेकार है।" ऐसा लगा कि वह उकसा रहा था।

मैं अभी लॉग ऑफ कर रहा हूँ। ये सब मेरे साथ ऐसा व्यवहार क्यों करते हैं?

-समीर

क्या आप बुलिंग के अलग अलग प्रकारों को पहचान सकते हैं? इन क्षणों का मिलान करें:

-एक्सक्लूशन: \_\_\_\_\_

-डॉक्सिंग: \_\_\_\_\_

-ट्रोलिंग: \_\_\_\_\_

यदि आप भी इस ऑनलाइन ग्रुप का हिस्सा होते तो आप क्या करते?



अब जब आप सभी ऑनलाइन गोपनीयता के बारे में जानते हैं, तो आइए ऑनलाइन दुनिया में कुछ खतरों के बारे में बात करते हैं - साइबरबुलिंग और उत्पीड़न के विभिन्न रूप। ये व्यवहार केवल "बुरे व्यवहार" नहीं हैं; वे गैरकानूनी और चोट पहुंचाने वाले हैं। लेकिन चिंता न करें! आप इन खतरों को समझकर अपनी ऑनलाइन सुरक्षा पर नियंत्रण रख सकते हैं।



साइबरस्टॉकिंग

साइबरस्टॉकिंग तब होता है जब कोई व्यक्ति आप पर ऑनलाइन नज़र रखता है आपकी पोस्ट चेक करता है, कमेंट्स करके परेशान करता है, या आपको असुरक्षित महसूस कराने के लिए मैसेज भेजता है।



यौन उत्पीड़न

ऑनलाइन यौन उत्पीड़न में अनुचित मैसेज, फोटो भेजना या शब्दों के माध्यम से किसी को असहज महसूस कराना शामिल है।



सेक्सटॉर्शन

सेक्सटॉर्शन तब होता है जब कोई व्यक्ति आपको निजी फोटो या वीडियो शेयर करने के लिए मजबूर करता है, फिर धमकी देता है कि अगर उन्हें पैसे नहीं दिए जायें और जो वो कह रहे हैं नहीं किया तो वे आपकी फोटो या वीडियो सबके साथ शेयर कर देंगे।



रिवेंज पोर्न

रिवेंज पोर्न तब होता है जब कोई व्यक्ति किसी अन्य व्यक्ति को शर्मिंदा करने या चोट पहुंचाने के लिए उसकी निजी तस्वीरें या वीडियो शेयर करता है।



कैटफिशिंग

कैटफिशिंग तब होती है जब कोई व्यक्ति दूसरों को धोखा देने या चोट पहुंचाने के लिए ऑनलाइन कोई और होने का दिखावा करता है। वे आपको धोखा देने के लिए नकली फोटो, नाम या विवरण का उपयोग कर सकते हैं।



मस्करेडिंग

मस्करेडिंग तब होती है जब कोई व्यक्ति आपको चोट पहुंचाने या हेरफेर करने के लिए किसी और का दिखावा करता है। यह कैटफिशिंग से थोड़ा अलग है, क्योंकि यह अक्सर नकली पहचान के पीछे छिपकर किसी को धमकाने या परेशान करने के लिए किया जाता है।



डीपफेक

डीपफेक तब होता है जब कोई व्यक्ति AI (कृत्रिम बुद्धिमत्ता) का उपयोग करके नकली फोटो या वीडियो बनाता है जो असली दिखते हैं लेकिन असली नहीं होते। इससे ऐसा लग सकता है कि किसी ने कुछ ऐसा कहा या किया जो उसने असल में नहीं किया।



अरे! यह तो सच में डरावना लगता है, भैया! मुझे मेरी क्लासमेट सारा की याद आ गई। उसने एक ऑनलाइन दोस्त बनाया था, जो उसे शुरुआत में गिफ्ट्स और फूल भेजता था। सारा को यह दोस्त बहुत पसंद था, और उसने उससे ऑफलाइन मिलना भी शुरू कर दिया। लेकिन अब वह अजीब महसूस करने लगी है क्योंकि वह आदमी उसे अकेले मिलने और और करीब आने के लिए कहने लगा है। वह 29 साल का है, और वह कहता है, "बड़े लोग ऐसे ही बिहेव करते हैं!" मुझे समझ नहीं आ रहा कि मैं सारा से क्या कहूं...

आह, मुझे बहुत खुशी है कि तुमने मुझे यह बताया, सुजैन। तुमने जो बताया वह एक और आम ऑनलाइन खतरा है - ग्रूमिंग। लेकिन चिंता मत करो, हम इसे एक साथ समझेंगे ताकि तुम अपनी दोस्त की अच्छे से मदद कर सको।



## ऑनलाइन ग्रूमिंग



ऑनलाइन ग्रूमिंग तब होती है जब कोई 18 साल से बड़ी उम्र का व्यक्ति किसी नाबालिग व्यक्ति को धोखा देकर या उसे बहला कर उसके साथ ऑनलाइन संबंध बनाता है। वे दोस्ताना और समझदार बनकर शुरुआत कर सकते हैं, लेकिन उनका असली लक्ष्य नाबालिग व्यक्ति का फ़ायदा उठाना और उसका यौन शोषण करना होता है।

## ऑनलाइन ग्रूमिंग के चरण

### पहचान

बच्चे से संपर्क करने से पहले, गूमर बच्चे को लक्ष्य बनाकर उसके जीवन के बारे में जानने का प्रयास कर सकते हैं, उसकी कमजोरियों की पहचान कर सकते हैं - बच्चे क्या चाहते हैं, वह किस बात से असंतुष्ट हैं, उन्हें क्या चाहिए और वह कैसा महसूस करते हैं।

### विश्वास जीतना

वे बच्चे की उन ज़रूरतों को पूरा करने की कोशिश करते हैं जो उनकी ज़िंदगी में और तरीकों से पूरी नहीं हो पातीं। अपराधी गिफ्ट देने, चापलूसी करने, पैसे देने और अन्य बुनियादी ज़रूरतों को पूरा करने जैसे हथकंडे अपनाते हैं।

### अकेला कर देना

वे बच्चों लिए अकेले रहने की परिस्थितियाँ पैदा करने की कोशिश हैं और बच्चे को इस बात पर विश्वास दिलाने की कोशिश करते हैं कि कोई भी बच्चे की उतनी परवाह नहीं करता जितना वे करते हैं। गूमर बच्चे की जिज्ञासा का फ़ायदा उठाकर उनके रिश्ते को शारीरिक भी बनाते हैं।

### नियंत्रण

यह यौन शोषण का रूप ले सकता है, जहां गूमर बच्चे पर नियंत्रण करने की कोशिश करता है—वह कहाँ जाए, क्या करे, किससे मिले, आदि। वह बच्चे को यह यकीन दिलाते हैं कि सिर्फ वही उसकी भावनात्मक और भौतिक ज़रूरतें पूरी कर सकते हैं।

## ग्रूमिंग के संकेत

**बहुत ज्यादा ध्यान देना:** यह व्यक्ति बच्चे को बार-बार तारीफें, गिफ्ट्स या खास ट्रीटमेंट देकर उसे खास महसूस कराता है, ताकि वह उस पर भरोसा करने लगे।

**अनुचित बातें करना:** ये लोग ऐसे टॉपिक्स पर बात करने लगते हैं जो बच्चे की उम्र के हिसाब से ठीक नहीं होते, जैसे रिश्ते या यौन विषयों पर जल्दबाजी में चर्चा करना।

**सीमाओं की परीक्षा लेना:** वे धीरे-धीरे शारीरिक या भावनात्मक सीमाओं को परखते हैं—जांचते हैं कि बच्चा कैसी प्रतिक्रिया देता है, और फिर धीरे-धीरे अपना बर्ताव और बढ़ाते हैं।

यह बिल्कुल वैसा ही लग रहा है जैसा सारा के साथ हो रहा है! अब उसे क्या करना चाहिए?



हां, तुम्हें सारा को तुरंत किसी भरोसेमंद बड़े के साथ मिलकर इस स्थिति की शिकायत संबंधित अधिकारियों से करने को कहना चाहिए। इसके अलावा चलो मैं तुम्हें भी ऐसी स्थिति में उठाने वाले कुछ ज़रूरी क़दमों के बारे में बताता हूँ!



3

## ग्रूमिंग के संकेतों को देखने पर क्या कार्रवाई की जानी चाहिए?

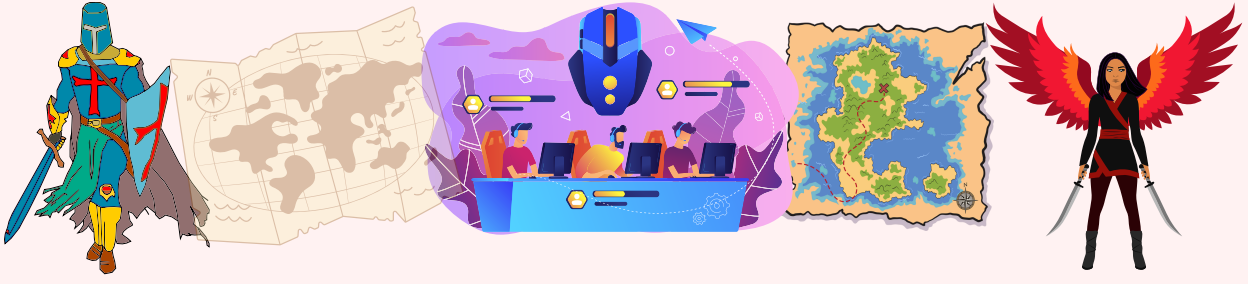
**सब कुछ लिखकर रखें:** जो भी बातचीत हो रही है, उसका रिकॉर्ड रखें। इसमें मैसेज या ईमेल के स्क्रीनशॉट, बातचीत के बारे में छोटे-छोटे नोट्स, और कोई भी ज़रूरी जानकारी शामिल हो सकती है।

**खुलकर बात करें:** किसी भरोसेमंद व्यक्ति से इस बारे में बात करें। यह माता-पिता, टीचर, स्कूल काउंसलर, या कोई और भरोसेमंद बड़ा व्यक्ति हो सकता है।

**बड़ों की मदद लें:** जिस बच्चे के साथ यह हो रहा है, उसे कहें कि स्थिति को बेहतर तरीके से संभालने के लिए भरोसेमंद बड़े व्यक्ति, जैसे माता-पिता, टीचर या स्कूल काउंसलर की मदद लें।

**धीरे-धीरे दूरी बनाएं:** बातचीत और मुलाकातों को धीरे-धीरे कम करें। मिलने के लिए शालीनता से से मना करें और मैसेज का जवाब देने में थोड़ा समय लें, ताकि सामने वाले को समझ आए कि आपको दूरी चाहिए।

# ऑनलाइन गेमिंग: मौज-मस्ती और जोखिम की दुनिया



रहीम शनिवार की दोपहर को मज़े से अपने भाई के लैपटॉप पर खेल रहा था, और पूरी तरह से एक ऑनलाइन गेम में डूबा हुआ था। उसने अभी-अभी एक कठिन स्टेज पार की थी और अपनी अगली चुनौती के लिए तैयार था, तभी उसे एक नोटिफिकेशन आया।

भैया, जब मैं गेम खेल रहा था तो कुछ अजीब हुआ। 'XxShadowSlayerxX' नाम का यह खिलाड़ी लगातार मेरा पीछा कर रहा था और मुझे मैसेज में कह रहा था, 'मुझे पता है तुम कहाँ रहते हो।' मैं इतना डर गया कि मैंने गेम बंद कर दिया और मेरी सारी प्रगति चली गई।

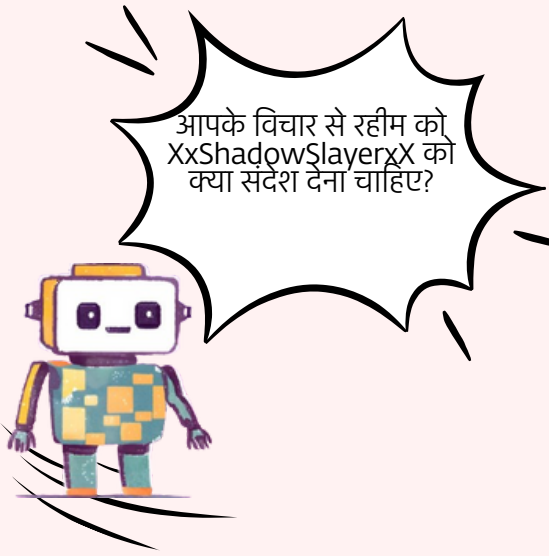
रहीम, यह साइबरस्टॉकिंग है। इसका उद्देश्य तुम्हें डराना है। तुमने इसे रोककर सही काम किया। अब, उसे तुरंत ब्लॉक करो और प्लेटफ़ॉर्म पर रिपोर्ट करो।

लेकिन अगर वह और भी कुछ करे तो क्या होगा? मुझे बहुत असुरक्षित महसूस हो रहा है।

अगर तुम सुरक्षित महसूस करते हैं तो आप अपना अकाउंट प्राइवेट बना सकते हो। और अजनबियों के साथ निजी जानकारी साझा करने से बचना बेहतर है। अगर ऐसा कुछ दोबारा होता है, तो तुरंत मेरे या किसी और भरोसेमंद बड़े के पास तुरंत जाना।

धन्यवाद भैया। मैं उसे ब्लॉक कर दूंगा और अपने दोस्तों को भी इस बारे में बताऊंगा।

गेमिंग मज़ेदार है, लेकिन इसमें जोखिम भी है। डीपफेक अवतारों से सावधान रहें, जहाँ खिलाड़ी कोई और होने का दिखावा करते हैं ताकि धोखे से आपकी व्यक्तिगत जानकारी ले सकें। ऑनलाइन गेमिंग तब हो सकती है जब कोई इन-गेम उपहारों के माध्यम से आपका विश्वास जीतता है, फिर व्यक्तिगत जानकारी मांगता है। और डॉक्सिंग से सावधान रहें, जहाँ खिलाड़ी आपको शर्मिंदा करने या धमकाने के लिए आपकी व्यक्तिगत जानकारी शेयर कर सकते हैं। हमेशा अपने व्यक्तिगत जानकारी को निजी रखें और कोई व्यवहार गलत लगने पर उसकी तुरंत रिपोर्ट करें।



**Chat**

XxShadowSlayerxX  
मैंने देखा तुमने यह चाल चली। हमेशा इतने धीरे खेलते हो क्या?

Rahim  
मैं बस गेम शुरू कर रहा हूँ।

XxShadowSlayerxX  
मेरे बिना कुछ कर नहीं सकते क्या? मेरा इंतज़ार कर रहे हो?

Rahim  
इतने सारे मैसेज क्यों भेज रहे हो? अपने गेम पर ध्यान दो।

XxShadowSlayerxX  
मैं तुम्हारी हर चाल जानता हूँ, तुम्हारे बारे में सब कुछ पता है।

Rahim  
...

**Send**

आपकी मदद से मैं फिर कभी ऐसी परिस्थितियों में डरा हुआ या कमज़ोर महसूस नहीं करूँगा। लेकिन भैया, मुझे बताओ, क्या ये खतरे सिर्फ़ ऑनलाइन गेमिंग के दौरान ही होते हैं?



बिल्कुल नहीं, रहीम। ये खतरे ऑनलाइन कहीं भी हो सकते हैं—सोशल मीडिया, वर्चुअल क्लास, यहाँ तक कि फैमिली चैट ग्रुप भी। जाने-पहचाने और अनजाने लोग हमारी सीमाओं का उल्लंघन कर सकते हैं। इसलिए ऑनलाइन दुनिया में हर जगह सतर्क रहना और अपनी गोपनीयता की रक्षा करना बहुत ज़रूरी है।



## आम ऑनलाइन खतरे : डिजिटल दुनिया में सुरक्षित रहें

कई बार लोग ऐसी जॉब एड्स देखते हैं जो कम मेहनत में ज्यादा पैसे कमाने का वादा करती हैं। ऐसे मौकों को देखकर वे जल्दी से अफ्लाई कर देते हैं और अपना नाम, ईमेल, और क्वालिफिकेशन जैसी ज़रूरी जानकारी शेयर कर देते हैं। फिर वेबसाइट एक "छोटी सी फीस" जमा करने को कहती है ताकि नौकरी पक्की हो सके। सब कुछ असली लगता है— और समझ आने तक बहुत देर हो जाती है। ठग पैसा लेकर गायब हो जाते हैं, और लोग बैठे अपनी जानकारी के गलत इस्तेमाल को ले कर परेशान होते रहते हैं।

ऐसी ऑनलाइन ठगी, नकली जॉब ऑफ़र, फ़िशिंग स्कैम, और गलत इरादों से की गई बातचीत (गूमिंग) आम हैं। और ये हमेशा अजनबियों तक ही सीमित नहीं होतीं—कई बार जाने-पहचाने लोग भी विश्वास तोड़ सकते हैं। इसलिए सतर्क रहना और अपने अंदर की आवाज़ सुनना ज़रूरी है। जब आप ऑनलाइन हों, तो ध्यान दें कि आपको सुरक्षित महसूस हो रहा है या नहीं। अगर कुछ अजीब लगे, तो सतर्क हो जाएं। आपकी समझदारी आपको डिजिटल दुनिया में सुरक्षित रहने में मदद कर सकती है।

## पीड़ित पर गोपनीयता उल्लंघन का प्रभाव

सारा के ऑनलाइन गूमिंग के अनुभव के बाद, सुजैन और उसकी कुछ सहपाठियों ने ऑनलाइन खतरों के बारे में चर्चा की। उन्होंने महसूस किया कि ऑनलाइन प्राइवैसी उल्लंघन और अन्य हमले आम हैं। चर्चा के बाद, सुजैन ने कुछ नोट्स बनाए और लिखा कि अलग-अलग लोग ऑनलाइन हमलों और प्राइवैसी उल्लंघन पर कैसे महसूस कर सकते हैं और प्रतिक्रिया दे सकते हैं।

यह सिर्फ उल्लंघन तक सीमित नहीं है—प्राइवैसी का उल्लंघन लोगों की ऑनलाइन दुनिया को लेकर भावनाओं को बुरी तरह प्रभावित कर सकता है। वे उन जगहों पर भरोसा खोने लगते हैं और दोबारा इस्तेमाल करने से हिचकिचाने लगते हैं। लेकिन यह सिर्फ इतना ही नहीं है। इसका असर हर व्यक्ति पर अलग तरीके से पड़ता है।

### सामाजिक और भावनात्मक

कुछ लोग इसे भावनात्मक रूप से महसूस करते हैं—जैसे चिंता या शर्मिंदगी, भले ही इसमें उनकी कोई गलती न हो। यह उन्हें असुरक्षित, बेबस और आहत महसूस करा सकता है। कभी-कभी वे इसके कारण खुद को सबसे दूर कर लेते हैं।

### भौतिक

कुछ लोगों पर इसका असर शारीरिक रूप से दिखता है। तनाव, नींद की परेशानी, भूख में बदलाव—कुछ को तो सेहत से जुड़ी समस्याएं भी होने लगती हैं।

यह हैरानी की बात नहीं है कि ध्यान लगाना भी मुश्किल हो जाता है। स्कूल के काम या यहां तक कि रोजमर्रा के कामों में दिक्कत होने लगती है। (सच कहें तो, समझ में आता है ऐसा क्यों!)

और हां, ये भावनाएं कुछ दिनों या हफ्तों बाद हल्की पड़ सकती हैं, लेकिन कुछ लोगों के लिए यह असर बहुत लंबे समय तक बना रहता है।

### हम क्या कर सकते हैं?

उनकी कहानियां सुनकर मुझे सच में सोचने पर मजबूर कर दिया। उन्होंने ऐसे लोगों से जुड़ाव महसूस किया जो उनकी स्थिति को समझ सकते थे, और इससे उन्हें थोड़ा सुकून मिला—जैसे यह सब सिर्फ उनकी गलती नहीं थी। बहुत दुख की बात है कि प्राइवैसी उल्लंघन ने उन्हें खुद पर शक करने पर मजबूर कर दिया, लेकिन इसका मतलब यह नहीं है कि वे कम सक्षम, भरोसेमंद या समझदार हैं। उनके साथ ऐसा नहीं होना चाहिए था, और यह याद रखने की जरूरत है कि किसी के साथ भी ऐसा नहीं होना चाहिए।



अगर आपकी या आपके किसी दोस्त की प्राइवैसी का उल्लंघन होता है, तो खुद को याद दिलाएं कि यह आपकी गलती नहीं है। चिंता, शर्मिंदगी या असुरक्षा जैसी भावनाओं को समझने और संभालने के लिए किसी भरोसेमंद व्यक्ति से बात करें।

स्वयं की देखभाल करके, खुद को ठीक होने का समय देकर, और ऐसे लोगों से जुड़े रहकर जो आपको हौसला दें, अपने सुधार और बेहतरी पर ध्यान दें।



आप कुछ समय के लिए ब्रेक ले सकते हैं और सुरक्षित आदतें सीखकर (जैसे मजबूत पासवर्ड का उपयोग करना या व्यक्तिगत जानकारी शेयर करने में सावधानी बरतना) धीरे-धीरे ऑनलाइन स्थानों पर फिर से विश्वास कर सकते हैं।

# खुद को सुरक्षित रखें: ऑनलाइन क्या शेयर करें

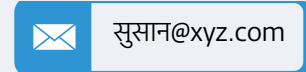
हमने अभी तक ऑनलाइन मौजूद कई तरह के खतरों को देखा, लेकिन आप अपनी प्राइवैसी को मजबूत करने और अपने डेटा पर नियंत्रण रखने के लिए कुछ कदम उठा सकते हैं! अब आइए इस पर ध्यान दें कि खुद को इन खतरों से कैसे बचाया जाए—यह समझकर कि ऑनलाइन क्या सुरक्षित है और क्या नहीं। आमतौर पर, इंटरनेट पर हमसे मांगी जाने वाली जानकारी तीन तरह की हो सकती है।

## व्यक्तिगत जानकारी

ऐसी जानकारी जो अजनबियों को सीधे या परोक्ष रूप से किसी व्यक्ति की पहचान करने में मदद कर सकती है—जैसे आपका नाम! यहां तक कि सामान्य लगने वाली छोटी-छोटी जानकारियां भी जोड़कर आपकी पहचान की पूरी तस्वीर बना सकती हैं।

व्यक्तिगत जानकारी के कुछ उदाहरण हैं:

- **बुनियादी जानकारी:** आपका पूरा नाम, जन्मतिथि या उम्र।
- **संपर्क जानकारी:** आपका फोन नंबर, घर का पता, ईमेल आईडी।
- **सोशल मीडिया गतिविधि:** लोकेशन टैग वाली तस्वीरें, किसी खास जगह पर चेक-इन, या ऐसी पोस्ट जिनसे आपकी पहचान हो सकती है।



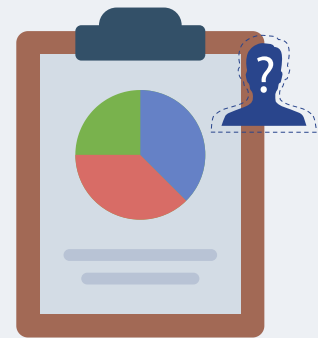
ऑनलाइन निजी जानकारी शेयर करने से पहचान की चोरी, पीछा करने या फ़िशिंग हमलों का जोखिम बढ़ जाता है। हमेशा निजी जानकारी शेयर करने से पहले दो बार सोचें, खासकर सार्वजनिक प्लेटफ़ॉर्म पर।

## गैर-व्यक्तिगत जानकारी

ऐसी जानकारी जिसका उपयोग किसी व्यक्ति की पहचान करने के लिए नहीं किया जा सकता - जैसे उसका पसंदीदा रंग! हालांकि यह सुरक्षित लग सकता है, लेकिन कभी-कभी गैर-व्यक्तिगत डेटा भी अन्य जानकारी के साथ मिलकर किसी व्यक्ति की पहचान करने में सहायक हो सकता है।

गैर-व्यक्तिगत जानकारी के कुछ उदाहरण हैं:

- **पसंद:** आपका पसंदीदा रंग, टीवी शो या शौक।
- **सामान्य राय:** किसी नई फिल्म या पुस्तक पर आपके विचार।
- **एकत्रित डेटा:** ट्रेंड या सर्वे परिणाम जो व्यक्तिगत जानकारी नहीं बताते।



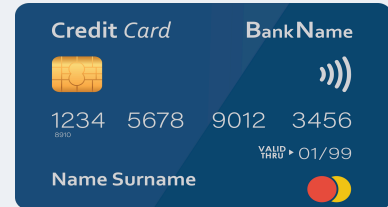
गैर-व्यक्तिगत जानकारी साझा करना आम तौर पर सुरक्षित होता है। पर सावधान रहें: आपकी पसंद या आदतें अभी भी लोगों को एल्गोरिदम या यहां तक कि बुरे व्यक्तियों को आपके व्यवहार के बारे में जानकारी दे सकती हैं।

## संवेदनशील व्यक्तिगत जानकारी

संवेदनशील व्यक्तिगत जानकारी – यानी ऐसी व्यक्तिगत जानकारी जो गलत इस्तेमाल के लिए और भी ज्यादा जोखिम में होती है, क्योंकि यह अन्य महत्वपूर्ण चीजों से जुड़ी होती है—जैसे आपकी हस्ताक्षर। इस जानकारी के दुरुपयोग से पैसों की धोखाधड़ी या पहचान की चोरी जैसी गंभीर समस्याएं हो सकती हैं।

संवेदनशील व्यक्तिगत जानकारी के कुछ उदाहरण:

- पहचान से जुड़ी जानकारी: आपका हस्ताक्षर, सरकार द्वारा जारी किए गए पहचान नंबर (जैसे आधार, पासपोर्ट, या सोशल सिक््योरिटी नंबर)।
- वित्तीय जानकारी: बैंक खाता नंबर, क्रेडिट/डेबिट कार्ड की जानकारी, या UPI पिन।
- सुरक्षा से जुड़ी जानकारी: पासवर्ड, पिन, सिक््योरिटी सवालों के जवाब, या बायोमेट्रिक डेटा (जैसे फिंगरप्रिंट या फेस रिकग्निशन)।
- स्वास्थ्य से जुड़ी जानकारी: मेडिकल रिकॉर्ड, बीमारियों की जानकारी, या डॉक्टर द्वारा लिखी गई दवाएं।



ज़रूरी है: संवेदनशील व्यक्तिगत जानकारी साइबर अपराधियों का मुख्य निशाना होती है। इसलिए, इसे सुरक्षित रखना बहुत ज़रूरी है और इसे केवल भरोसेमंद संस्थानों के साथ सुरक्षित प्लेटफॉर्म पर ही शेयर करना चाहिए।

## गतिविधि

मीरा को यह तय करने में मदद करें कि कौन सी जानकारी ऑनलाइन शेयर करना सुरक्षित है। नीचे दी गई स्थितियाँ और जानकारी के प्रकारों को पढ़ें और:

- जानकारी के प्रकार की पहचान करें

व्यक्तिगत

गैर-व्यक्तिगत

संवेदनशील व्यक्तिगत

- मीरा का कार्य तय करें

बिना डरे शेयर करें

शेयर करने से बचें

सावधानी से शेयर करें (केवल आवश्यक होने पर और विश्वसनीय प्लेटफॉर्म पर)

परिदृश्य:

मीरा को एक ऑनलाइन पहली-सुलझाने की प्रतियोगिता में शामिल होने के लिए अपना पूरा नाम अपलोड करने के लिए कहा गया।

प्रकार: \_\_\_\_\_

क्या करें: \_\_\_\_\_

एक कुकिंग ऐप ने मीरा से उनकी रेसिपी भेजने के लिए उनका ईमेल एड्रेस मांगा।

- प्रकार: \_\_\_\_\_
- क्या करें: \_\_\_\_\_

एक अनजानी वेबसाइट ने मीरा से एक प्रतियोगिता में भाग लेने के लिए उसका फोन नंबर मांगा।

प्रकार: \_\_\_\_\_  
क्या करें: \_\_\_\_\_

एक गेमिंग ऐप मीरा की उम्र पता करने के लिए उसकी जन्मतिथि जानना चाहता है।

प्रकार: \_\_\_\_\_  
क्या करें: \_\_\_\_\_

मीरा ने एक चर्चा मंच पर अपनी पसंदीदा किताब का शीर्षक साझा किया।

प्रकार: \_\_\_\_\_  
क्या करें: \_\_\_\_\_






एक शॉपिंग वेबसाइट मीरा से डिलीवरी के लिए उसका पता मांगती है।

प्रकार: \_\_\_\_\_  
क्या करें: \_\_\_\_\_

मीरा को ऑनलाइन बैंकिंग सेवा के लिए अपनी पहचान बताने के लिए अपना हस्ताक्षर अपलोड करने के लिए कहा जाता है।

प्रकार: \_\_\_\_\_  
क्या करें: \_\_\_\_\_

## याद रखें: ऑनलाइन जानकारी शेयर करते समय कैसे सुरक्षित रहें

-  शेयर करने से पहले सोचें: हमेशा यह प्रश्न करें कि क्या जानकारी वास्तव में ऑनलाइन शेयर करना आवश्यक है।
-  दृश्यता सीमित करें: सोशल मीडिया पर गोपनीयता सेटिंग का उपयोग करके तय करें कि आपकी पोस्ट कौन देख सकता है।
-  सार्वजनिक वाई-फाई पर सावधान रहें: सार्वजनिक या असुरक्षित नेटवर्क से कनेक्ट होने पर संवेदनशील जानकारी शेयर करने से बचें।
-  सुरक्षित चैनलों का उपयोग करें: संवेदनशील जानकारी (जैसे, बैंक जानकारी) केवल एन्क्रिप्टेड प्लेटफ़ॉर्म पर ही शेयर करें।
-  खातों की नियमित निगरानी करें: किसी भी दुरुपयोग को जल्दी पकड़ने के लिए अपने ऑनलाइन खातों पर असामान्य गतिविधि के लिए नजर रखें।



# चैप्टर 4: सोचें, समझें, फिर क्लिक करें: मिसइन्फॉर्मेशन से बचने के टिप्स



**BREAKING NEWS**

बोर्ड की परीक्षाएं  
रद्द कर दी गई हैं!

छात्रों के लिए एक  
जरूरी खबर

बड़े पैमाने पर  
साझा करें!

शुभम अपने फोन पर स्करोल कर रही थी, तभी उसे एक जरूरी खबर मिली। उसने तुरंत इसे अपने सोशल मीडिया पर शेयर कर दिया ताकि लोग इसे जान सकें।



अरे शुभम, मुझे लगता है कि यह झूठी खबर है!

थोड़ा सावधान रहो, इसे कल ही गलत साबित कर दिया गया था।



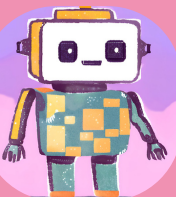
यह सच नहीं है, शुभम। मैंने अभी एक लेख पढ़ा जिसमें इस पर सफाई दी गई है!

जल्द ही, शुभम को अपने शेयर किए गए पोस्ट पर ढेर सारे कमेंट्स मिल जाते हैं।

क्या? नहीं! ये फ्रैक कैसे हो सकता है, ये तो बिल्कुल असली लग रहा था! सिद्धार्थ, ज़रा देखो - मैंने ये न्यूज़ अपने प्रोफाइल पर शेयर कर दी, और अब लोग कह रहे हैं कि ये झूठी है! मुझे समझ नहीं आ रहा क्या करूं, लोग मेरा मज़ाक उड़ाएंगे!

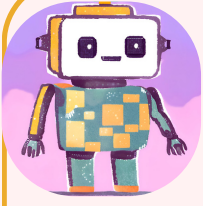


चिंता मत करो, यह सिर्फ तुम्हारे साथ नहीं है शुभम! मेरे कुछ और दोस्तों को भी हाल ही में इसी समस्या का सामना करना पड़ा। ऐसा लगता है कि तुम गलत जानकारी के जाल में फंस गई हो। मुझे सब कुछ तो नहीं पता, लेकिन शायद हम मिलकर ऑनलाइन जानकारी को समझने का तरीका ढूंढ सकें?



मिशन NIO में आपका स्वागत है: Navigate Information Online यानी ऑनलाइन जानकारी को नेविगेट करें। अब न्यूज़ नेविगेटर बनने का सही समय है!

## गतिविधि



क्या आपने कभी ऑनलाइन कुछ शेयर किया है, यह सोचकर कि यह सच है, लेकिन बाद में पता चला कि यह सच नहीं है? आपको यह कैसे पता चला? अगली बार आप क्या अलग करेंगे?

एक पल के लिए सोचिए और अपने विचार नीचे दिए गए स्थान में लिख दीजिए।



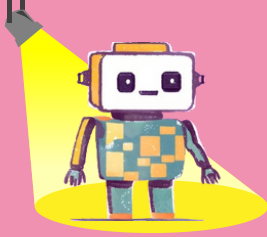
अमित भैया, हम कैसे पता कर सकते हैं कि कोई चीज़ असली है या नकली? इंटरनेट पर तो बहुत सारी जानकारी है!



यह तो बहुत अच्छा सवाल है! इसे समझने के लिए, सबसे पहले हमें यह जानना होगा कि ऑनलाइन कौन-कौन सी जानकारी उपलब्ध है और उनका मकसद क्या है।



## ऑनलाइन जानकारी के प्रकार



मैं तुम्हें इसे समझाता हूँ! शुभम, चलो मिलकर तुम्हारे सोशल मीडिया न्यूज़फ़ीड पर एक नज़र डालते हैं। जल्द ही, तुम देखोगी कि ऑनलाइन जानकारी आमतौर पर इन प्रकार की होती है:



### सत्यापित और विश्वसनीय जानकारी

कुछ खबरें या जानकारियाँ मशहूर न्यूज़ चैनलों, रिसर्च संगठनों या सरकारी वेबसाइटों से आती हैं। ये आमतौर पर फैक्ट-चेक की हुई और भरोसेमंद होती हैं।

### राय और व्यक्तिगत जानकारी

ऐसा कंटेंट किसी व्यक्ति का नज़रिया दिखाता है - जैसे कि ब्लॉग, पोस्ट या पर्सनल वीडियो जर्नल, जो किसी की रोज़मर्रा की जिंदगी, भावनाएँ और राय दर्शाते हैं। ये ज़रूरी नहीं कि हमेशा तथ्यों पर आधारित हों।

### गलत जानकारी, भ्रामक जानकारी और नकली खबरें

झूठी जानकारी के अलग-अलग रूप हैं। इनमें अक्सर चौंकाने वाली हेडलाइंस, भावनात्मक भाषा, अस्पष्ट स्रोत और जल्दी भरोसा दिलाने का दबाव होता है।

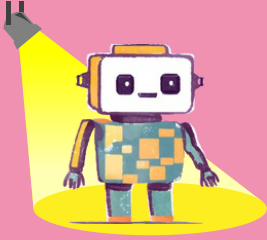
### हास्य और मनोरंजन

इंटरनेट पर ऐसे मजेदार चुटकुले और मीम्स भरे पड़े हैं जिन्हें लोग समाचार की तरह ले लेते हैं - खासकर जब वे असली घटनाओं या मुद्दों पर बात करते हैं।

ओह... तो इंटरनेट पर जो कुछ भी है वो हमेशा सच या गंभीर नहीं होता! तो अब मैं समझी!



बिल्कुल सही! थोड़ी कोशिश करके जब तुम जानकारी के अलग-अलग प्रकारों में फर्क करना सीख जाओगी, तो आप इंटरनेट पर समझदारी से काम कर पाओगी!



आइए शुभम के न्यूज़फ़ीड से कुछ और पोस्ट और इस हफ़्ते उसे मिले मैसेजएस पर नज़र डालते हैं। क्या आप बता सकते हैं कि हर जानकारी किस प्रकार की है?



हेलो शुभम! मैंने अभी पढ़ा कि वैज्ञानिकों ने अल्जाइमर के इलाज में कुछ प्रगति की है! मैं यह बात आपसे साझा करना चाहता था क्योंकि आप अपनी दादी के लिए रिसर्च कर रहे थे।

चूँकि मैं अल्जाइमर रोग के इलाज के लिए साँस के जरिए लिया जाने वाला जेनॉन माइक्रोग्लिया का इस्तेमाल:

<https://www.science.org/doi/10.1126/scitranslmed.adk3690>



>> कई बार भेजा गया

फ्लाइंग अटेंडेंट ने प्रथम श्रेणी में सुंदर पिचाई का अपमान किया - सच्चाई जानकर आप हैरान रह जाएंगे!

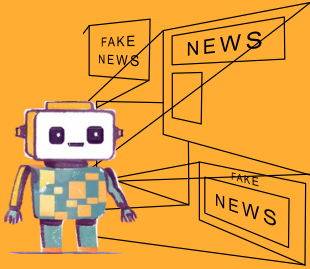
और पढ़ें...

## गलत जानकारी की पहचान

भैया, अभी भी एक दिक्कत है! मजेदार पोस्ट में झूठी जानकारी पहचानना तो आसान है, लेकिन जब पोस्ट गंभीर होती है, तो मैं कैसे जानूँ कि वो सच है या नहीं?



बहुत बढ़िया सवाल! ग्लिच झूठी जानकारी पकड़ने में माहिर है और तुम्हें इसके अलग-अलग प्रकार और पहचानने के संकेत दिखा सकता है!



वर्ल्ड वाइड वेब स्कैन किया जा रहा है... ऑनलाइन जानकारी सोशल मीडिया, न्यूज़ साइट्स, प्राइवेट मैसेजेस जैसी कई जगहों से होकर गुज़रती है—और हर स्टाप पर यह बदल सकती है! हर झूठी जानकारी एक जैसी नहीं दिखती, लेकिन इसके तीन मुख्य प्रकार होते हैं...

### 1. गलत जानकारी

अनजाने में शेयर की गई गलत या भ्रामक जानकारी - यानी, भेजने वाले को यह नहीं पता कि जानकारी गलत है।



शायद यह मैसेज भेजने वाला व्यक्ति छात्रों को भ्रमित करने की कोशिश कर रहा है, शुभम!

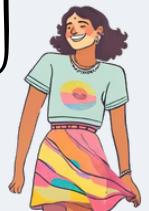
जैसे मैंने गलती से परीक्षा रद्द होने की गलत जानकारी शेयर कर दी थी!



### 2. भ्रामक जानकारी

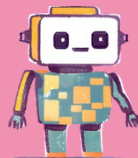
ऐसी जानकारी जो लोगों को भ्रमित करने के लिए होती है - आमतौर पर, राजनीतिक, वित्तीय या सामाजिक फायदे के लिए।

ऐसा लग रहा था कि यह किसी न्यूज़ साइट पर था - इसलिए मैंने इस पर भरोसा कर लिया...



### 3. झूठी खबरें

जब झूठी जानकारी को खबर के तौर पर बाँटा जाता है - ताकि वो सही लगे।



...कभी-कभी एक ही जानकारी इन तीनों प्रकारों में शेयर की जा सकती है!

## गतिविधि



फर्जी खबर, गलत जानकारी या गलत सूचना का कोई उदाहरण बताएं जो आपने पहले देखा हो। आपको कैसे पता चला कि यह सच नहीं है? जो आप पहले से जानते हैं, वह वाकई में मददगार हो सकता है!

---



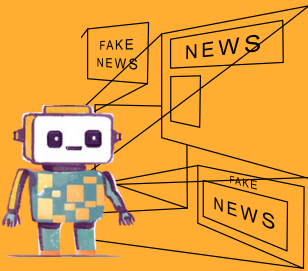
---



---



---



आप सूचना या समाचार की सच्चाई का पता लगाने के लिए कई तरीकों का इस्तेमाल कर सकते हैं। एक आसान और याद रखने में सरल तरीका है SUCS विधि, जिसका मतलब है स्रोत (Source), सभी जगह मौजूद होना (Ubiquity), संदर्भ (Context) और दूसरी राय (Second Opinion)। यह आपको यह समझने में मदद करेगा कि आपको यह सुनिश्चित करने के लिए किन बातों पर ध्यान देना चाहिए कि आप ऑनलाइन केवल विश्वसनीय जानकारी पर भरोसा कर रहे हैं! चलिए, हम हर एक चरण को ध्यान से देखते हैं और इन दो समाचारों की सच्चाई का पता लगाने की कोशिश करते हैं:

https://इकोनॉमिकटाइम्स.इंडियाटाइम्स.com/news/budget-2025

घर ताजा खबर बाजार अर्थव्यवस्था राजनीति चुनाव समाचारों का क्लॉक

### द इकोनॉमिक टाइम्स

स्वास्थ्य मंत्रालय की फंडिंग के ताजा अपडेट

डॉ. सोहिनी कुमार के द्वारा | आखिरी बार 22 फरवरी 2022 को अपडेट किया गया



नई दिल्ली: सत्तारूढ़ पार्टी अगले राज्य चुनावों की तैयारी कर रही है, जबकि स्वास्थ्य मंत्रालय ने अपने राष्ट्रीय स्वास्थ्य मिशन के लिए महत्वपूर्ण कटौती की है, जो अस्पतालों में आपूर्ति की कमी का सामना कर रहे 50% राज्यों की स्थिति को प्रभावित कर सकती है। विपक्ष ने...

लेखक के बारे में:

डॉ. सोहिनी कुमार स्कूल ऑफ इकोनॉमिक्स एंड बिजनेस में प्रोफेसर हैं और एक दशक से ज्यादा से भारतीय स्वास्थ्य प्रणालियों और राजनीति का अध्ययन कर रही हैं।

बढ़िया! तो चलो शुरू करें!



आपको क्या लगता है? क्या ये खबर सही लगती है?



http://इकोनॉमिक्समेडीज़ी123.बिज़/इंडिया-टू-पे-फॉरेन-

### इकोनॉमिक्समेडीज़ी

भारत निजी नागरिक बैंक खातों में हस्तक्षेप करके विदेशी ऋण चुकाएगा!!

भारत को विदेशी देशों से भारी कर्ज मिल रहा है और राष्ट्रीय खजाना तेजी से खाली होता जा रहा है। राज्यों के पास पैसे की कमी है और इस खर्च को पूरा करने का एकमात्र तरीका नागरिकों के बैंक खातों से सीधे पैसे निकालना है। निजी बैंकों ने पहले ही इस योजना से बाहर निकलने का ऐलान कर दिया है, लेकिन सरकारी बैंकों में कोई भी खाता अब दुरुपयोग से सुरक्षित नहीं है... (और पढ़ें)

अभी रम्मी खेले और 10,000 रुपये जीतें!!





चित्र: भारत के विदेश सचिव एक नए निजी बैंक के मालिक से हाथ मिलाते हुए



## स्रोत

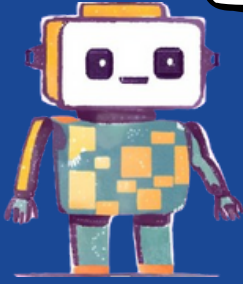
सबसे पहला कदम है जानकारी या समाचार के स्रोत की जांच करना। क्या यह भरोसेमंद है? क्या आप उस स्रोत पर विश्वास कर सकते हैं?

मतलब, मुझे देखना चाहिए कि इसे पोस्ट किसने किया? लेकिन मुझे तो न्यूज़ आमतौर पर भरोसेमंद दोस्तों से फॉरवर्ड मिलती है...



शायद बात असली स्रोत की भी है – जैसे न्यूज़ चैनल, रिसर्च स्टडीज़ या आधिकारिक बयान। हमें इन्हें भी चेक करना होगा, लेकिन कैसे?

इस चेकलिस्ट का इस्तेमाल करो!  
अगर ज्यादातर बातें सही लगती हैं, तो जानकारी भरोसेमंद हो सकती है। लेकिन अगर शक हो, तो न्यूज़ फॉरवर्ड मत करो!



हमेशा गौर से देखो



## जांच की सूची

- क्या वेबसाइट एक मशहूर न्यूज़ चैनल, शोध पत्रिका या प्रतिष्ठित संगठन की है?
- क्या यह वेबसाइट सही और जांची-परखी जानकारी देने के लिए जानी जाती है?
- क्या URL सुरक्षित है? (जैसे, 'https' से शुरू हो और आपका ब्राउज़र इसे असुरक्षित न बताए)
- क्या वेबपेज साफ-सुथरा और प्रोफेशनल दिखता है? (बेवजह के पॉप-अप ऐड, गलतियाँ या अजीब डिज़ाइन न हो)
- क्या लेखक भरोसेमंद और इस विषय का जानकार है? (क्या उन्होंने पहले भी इस पर स्टडी की है और सच बताया है?)

# आइए जाँच करें

चलिए, अपने लेखों पर लौटते हैं। क्या उनके स्रोत भरोसेमंद हैं?



वेबसाइट सुरक्षित URL का उपयोग करती है जो https से शुरू होता है।

इकोनॉमिक टाइम्स एक प्रतिष्ठित समाचार वेबसाइट है, जो विश्वसनीय और सटीक जानकारी देने के लिए मशहूर है।

लेखक इस विषय पर लिखने के लिए सक्षम है।

कुल मिलाकर, वेब-पेज साफ और अच्छे से डिज़ाइन किया गया है, इसमें कोई विज्ञापन, पॉप-अप या व्याकरण की गलतियाँ नहीं हैं।

वेबसाइट का यूआरएल सुरक्षित नहीं है! यह http (बिना "s" के) से शुरू होता है, और इसमें कुछ वर्तनी की गलतियाँ और असंगतियाँ हैं। यह .biz पर भी खत्म होता है।



यह वेबसाइट अविश्वसनीय और अनौपचारिक है, और हमें नहीं पता कि इसकी जानकारी सही और भरोसेमंद है या नहीं!

कोई लेखक नहीं है!

वेबसाइट पर बड़े-बड़े पॉप-अप और विज्ञापन हैं, और इसमें फॉर्मेटिंग और ग्रामर से जुड़ी कुछ समस्याएँ और असंगतियाँ भी हैं!

अभी रम्मी खेलें और 10,000 रुपये जीतें!!



सुझाव: टैब्लॉयड, फ्लायर्स, मैसेज बोर्ड, सोशल मीडिया पोस्ट, ब्लॉग और वेबसाइट्स जो बहुत कम लोगों को पता हैं, वे अक्सर अविश्वसनीय स्रोत होते हैं!

## गतिविधि



विश्वसनीय साइटों के तीन उदाहरण और आपके सामने आई अविश्वसनीय साइटों के तीन उदाहरण बताएं।

---



---



---



---

यह बहुत बढ़िया टिप है, अब मैं ध्यान दूंगा कि मेरी न्यूज़ कहाँ से आ रही है!



तुम ज़िम्मेदार नेटिजन बनने की राह पर हो - लेकिन सिर्फ़ स्रोत देखना ही काफ़ी नहीं है!



## सभी जगह मौजूद होना

इसका मतलब है कि यह जानकारी हर जगह मौजूद है। क्या जानकारी सिर्फ़ एक जगह है या इसे अलग-अलग स्रोतों से चेक किया जा सकता है? क्या कई विश्वसनीय स्रोतों ने इसकी रिपोर्ट की है और इसकी पुष्टि की है?

रुको, मुझे यह समझ नहीं आया। यह इतना ज़रूरी क्यों है? क्या कभी-कभी झूठी खबरें तेज़ी से नहीं फैलती?



सच है: सिर्फ़ इसलिए कि कई वेबसाइट्स ने कोई दावा किया है, इसका मतलब ये नहीं कि वो सच ही हो! लेकिन कुछ मामलों में - खासतौर पर भ्रामक जानकारी में - न्यूज़ को ऐसा बनाया जाता है कि लोग घबरा जाएं। सोचो अगर तुम्हें ऑनलाइन या किसी मैसेज में ये हेडलाइंस दिखें:

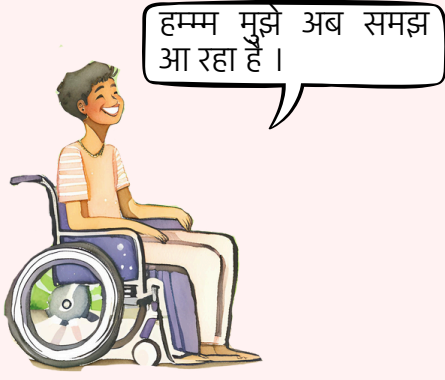


खतरा: 5G नेटवर्क पूरी दुनिया में COVID-19 वायरस के फैलने के लिए ज़िम्मेदार है!

ज़रा सोचिए: अगर पूरे देश में कुछ इतना खतरनाक हो रहा होता, तो ज़्यादा न्यूज़ साइट्स उसे कवर करतीं। राष्ट्रीय और अंतरराष्ट्रीय संगठन तुरंत इसकी जांच करते, शिकायतें दर्ज की जातीं और आधिकारिक बयान जारी किए जाते...

नमक में मिला जानलेवा सायनाइड: भारत में दुकानों पर घरों में बेचा जा रहा है यह ज़हर

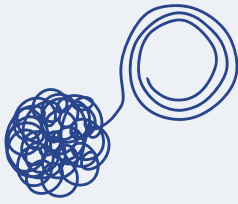
अगर इनमें से कुछ भी नहीं मिल रहा है, और ये खबरें सिर्फ़ ऑनलाइन कुछ अनजान जगहों पर हैं, तो यह कहना सही होगा कि ये शायद सच नहीं हैं।



लेकिन तुम सही कह रहे हो! सबसे भरोसेमंद स्रोत भी कभी-कभी गलतियाँ कर सकते हैं, इसलिए खुद से जानकारी जांचना हमेशा अच्छा होता है...



## सन्दर्भ



स्वतंत्र रूप से यह जाँच करें कि जानकारी का संदर्भ उस संदर्भ से मेल खाता है जिसमें इसे दिखाया जा रहा है।

चलो इसे समझते हैं! क्या तुम्हारे साथ कभी ऐसा हुआ है कि कोई चीज़ गलत संदर्भ में पेश की गई हो? तुमने कुछ और समझा, लेकिन असल में वो कुछ और ही निकला?



मुझे एक मैसेज मिला जिसमें नॉर्थ कोरिया के नेता किम जोंग उन की तस्वीर थी, और उसे चीन का राष्ट्रपति बताया जा रहा था। लेकिन असल में चीन के राष्ट्रपति शी जिनपिंग हैं!



पिछले महीने सुरक्षा नगर में सभी घबरा गए क्योंकि एक मैसेज में भूकंप की चेतावनी दी गई थी... लेकिन वो वीडियो सात साल पुराना था, और वो भी नेपाल का!



बढ़िया उदाहरण। दुर्भाग्य से, यह काफी सामान्य है, लेकिन आप लोग बहुत समझदार हैं! कल मुझे एक वीडियो मिला, जिसमें लगा कि दीपिका पादुकोण कोई कॉन्टेस्ट अनाउंस कर रही हैं! लेकिन वो AI से एडिट किया गया था ताकि ऐसा लगे कि वही बोल रही हैं!



सिद्धार्थ, अमित भैया, चलो मिलकर एक चेकलिस्ट बनाते हैं कि हमें क्या-क्या वेरिफाई करना चाहिए!





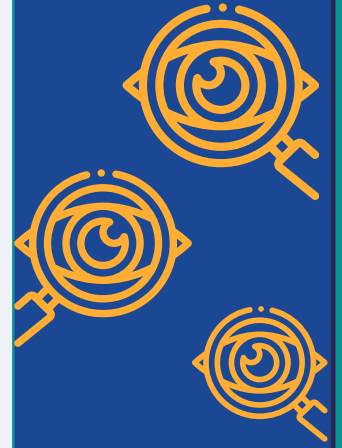
अच्छा आईडिया है

एक और ज़रूरी बात याद रखना: हमें पूरी कहानी सही तरीके से बतानी चाहिए, बिना कोई जानकारी छिपाए, उसका मतलब बदले या गलत तरीके से पेश किए!



## जांच की सूची

- क्या नाम, स्थान और तिथियां स्पष्ट और सही हैं, बजाय इसके कि एक चीज को दूसरी चीज के रूप में दिखाया जाए?
- क्या जानकारी अपडेटेड है?
- क्या महत्वपूर्ण जानकारी को छोड़ने के बजाय, पूरे संदर्भ को सबूत के साथ समझाया गया है?
- क्या सूचना में दिए गए फोटोज़ और वीडियो एक ही व्यक्ति, स्थान या घटना के हैं?
- क्या फोटो और वीडियो को बिना काटे, एडिट या गुमराह किए बिना सटीक रूप से पेश किया गया है?
- क्या इसमें जानबूझ कर उन दृष्टिकोणों को नजरअंदाज किया गया है जो हमें स्थिति को बेहतर तरीके से समझने में मदद कर सकते हैं?



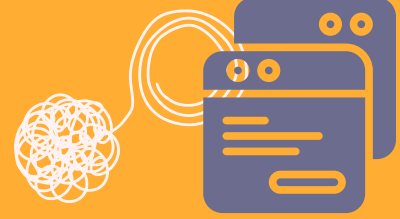
सुझाव: जिस साइट पर आप हैं, वहाँ से बाहर निकलकर अन्य स्रोतों से संदर्भ की जांच करें - बेहतर होगा कि आप असल स्रोत पर जाएँ और दिए आगे मुद्दे को बेहतर समझें!



संदर्भ को देखते समय, यह ध्यान रखें कि आप जिस लेख, पोस्ट या मैसेज को देख रहे हैं, वह क्या अध्ययन, रिपोर्ट, रिकॉर्डिंग या दस्तावेजों के लिंक के जरिए सबूत पेश करता है। क्या यह आपको बताता है कि जानकारी कैसे प्राप्त की गई? क्या सबूत विश्वसनीय और भरोसेमंद है?

## आइए जाँच करें!

चलिए, अपने लेखों पर लौटते हैं। क्या जानकारी और उसे पेश करने का तरीका उसके संदर्भ के हिसाब से सही है?



लेख में स्थान और तारीख का साफ-साफ जिक्र है, और जानकारी ताज़ा है।

लेख में प्रमाण के साथ मुद्दे का संदर्भ दिया गया है, और अन्य साइटों पर भी इसी तरह की जानकारी उपलब्ध है।

छवि राष्ट्रीय स्वास्थ्य मिशन के संदर्भ से मेल खाती है और छवि बिना किसी एडिटिंग या बदलाव के आधिकारिक है।

इसमें कोई डेट, जगह या लेखक नहीं है!

इस बात का कोई संदर्भ नहीं है कि यह कर्ज किस देश या बैंक से जुड़ा है! इतनी बड़ी खबर होने के बावजूद किसी और समाचार साइट ने इस कहानी को नहीं छापा है!

इस तस्वीर का उपयोग सही संदर्भ या सही कैप्शन के बिना किया गया है! यह ब्रिटिश विदेश सचिव द्वारा युवा पेशेवरों के लिए एक योजना शुरू करने के लिए भारतीय विदेश मंत्री से मिलने की तस्वीर है!

द इकोनॉमिक टाइम्स  
स्वास्थ्य मंत्रालय के फंडिंग के ताजा अपडेट

डॉ. सोहिनी कुमार के द्वारा | आखिरी बार 22 फरवरी 2022 को अपडेट किया गया

नई दिल्ली: सत्तारूढ़ पार्टी अगले राज्य चुनावों की तैयारी कर रही है, जबकि स्वास्थ्य मंत्रालय ने अपने राष्ट्रीय स्वास्थ्य मिशन के लिए महत्वपूर्ण कटौती की है, जो अस्पतालों में आपूर्ति की कमी का सामना कर रहे 50% राज्यों की स्थिति को प्रभावित कर सकती है। विपक्ष ने...

लेखक के बारे में:  
डॉ. सोहिनी कुमार स्कूल ऑफ इकोनॉमिक्स एंड बिजनेस में प्रोफेसर हैं और उन्होंने भारतीय स्वास्थ्य प्रणालियों और राजनीति का अध्ययन एक दशक से ज्यादा समय तक किया है।

इकोनॉमिक्समेडैज़ी  
भारत निजी नागरिक बैंक खातों में हस्तक्षेप करके विदेशी ऋण चुकाएगा!!

भारत को विदेशी देशों से भारी कर्ज मिल रहा है और राष्ट्रीय खजाना तेजी से खाली होता जा रहा है। राज्यों के पास पैसे की कमी है और इस खर्च को पूरा करने का एकमात्र तरीका नागरिकों के बैंक खातों से सीधे पैसे निकालना है। निजी बैंकों ने पहले ही इस योजना से बाहर निकलने का ऐलान कर दिया है। लेकिन सरकारी बैंकों में कोई भी खाता जब दुरुपयोग से सुरक्षित नहीं है... (और पढ़ें)

चित्र: भारत के विदेश सचिव एक नए निजी बैंक के मालिक से हाथ मिलाते हुए

अभी रम्मी खेलें और 10,000 रुपये जीतें!!

## यहाँ कुछ और खबरें हैं: क्या आप बता सकते हैं कि ये क्यों भ्रामक हैं?

@8pmgyan  
"अगर पाकिस्तान कोरोना वैक्सीन विकसित करता है, तो वह इसे कभी भी इजराइल या भारत को नहीं देगा।" पाक प्रधानमंत्री इमरान खान।

"अगर पाकिस्तान कोरोना वैक्सीन विकसित करता है, तो वह इसे कभी भी इजराइल या भारत को नहीं देगा।" - पाक प्रधानमंत्री इमरान खान।

क्या पाकिस्तान वैक्सीन बना सकता है?  
क्या इजराइल इस बात से सहमत है? 8pmGyan

भारत के सहयोग से नासा ने गैर-मानवों द्वारा बनाए गए फसल चक्रों की पुष्टि की है। अब सभी पश्चिमी देश भारत की महानता के आगे झुक रहे हैं!!

@नागरिक मंच  
सेंट्रल हॉस्पिटल में अब दिन के आखिरी 50 कोविड-19 टीके बांटे जा रहे हैं। विशेषज्ञों का कहना है कि अगले एक हफ्ते तक कोई और टीका नहीं आएगा!



## दूसरी राय लेना

अगर आप अभी भी पूरी तरह से दी गई जानकारी पर भरोसा नहीं कर सकते हैं, तो किसी विशेषज्ञ या तथ्य-जांचने वाली वेबसाइट जैसे ऑनलाइन संसाधन से दूसरी राय लेना हमेशा फायदेमंद हो सकता है।

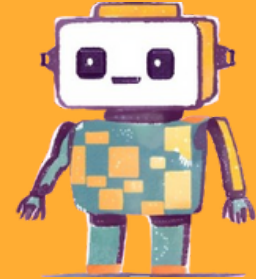


तथ्य-जांच करने वाली वेबसाइट? ये क्या होती हैं?!

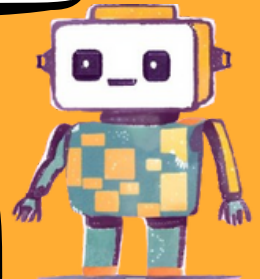
तथ्य-जांच वेबसाइटें इंटरनेट पर फैलने वाली फर्जी खबरों और गलत सूचनाओं को पहचानने के लिए बनी हैं।



लेकिन उन्हें कैसे पता चलेगा कि यह असली नहीं है?



बढ़िया सवाल है! हर साइट की अपनी तकनीक होती है, जिसे वे अपनी वेबसाइट पर समझाते हैं। आमतौर पर, जानकारी असल में ऑनलाइन आई कहाँ से ये पता लगाने के लिए एडवांस वेब खोज की जरूरत होती है...



वे मूल स्रोतों को पढ़ते और देखते हैं, और वेरीफाई करने के लिए स्थानीय प्राधिकारियों या समाचार में शामिल लोगों से बात करते हैं... यहाँ तक की दूसरी राय के लिए हम विशेषज्ञों से भी संपर्क कर सकते हैं!



## आइए जाँच करें!

चलिए, अपने लेखों पर लौटते हैं। उनके लिए दूसरी राय के कुछ स्रोत क्या हो सकते हैं? आप किससे बात कर सकते हैं?



https://इकोनॉमिक्स.इंडिया.कॉम/news/budget-2025

घर ताज़ा खबर बाज़ार अर्थव्यवस्था राजनीति चुनाव समाचारों का ब्लॉग

### द इकोनॉमिक्स टाइम्स

स्वास्थ्य मंत्रालय के फंडिंग के ताज़ा अपडेट

डॉ. सोहिनी कुमार के द्वारा | आखिरी बार 22 फरवरी 2022 को अपडेट किया गया



नई दिल्ली: सत्तारूढ़ पार्टी अगले राज्य चुनावों की तैयारी कर रही है, जबकि स्वास्थ्य मंत्रालय ने अपने राष्ट्रीय स्वास्थ्य मिशन के लिए महत्वपूर्ण कटौती की है, जो अस्पतालों में आपूर्ति की कमी का सामना कर रहे 50% राज्यों की स्थिति को प्रभावित कर सकती है। विपक्ष ने...

लेखक के बारे में:  
डॉ. सोहिनी कुमार स्कूल ऑफ इकोनॉमिक्स एंड बिजनेस में प्रोफेसर हैं और उन्होंने भारतीय स्वास्थ्य प्रणालियों और राजनीति का अध्ययन एक दशक से ज्यादा समय तक किया है।

### स्वास्थ्य मंत्रालय की साइट

---

---

---

---

### टाइम्स ऑफ इंडिया स्कूल के शिक्षक

---

---

---

http://इकोनॉमिक्समेडीज़ी123.बिज़/इंडिया-टू-पे-फॉरेन-

### इकोनॉमिक्समेडईज़ी

भारत निजी नागरिक बैंक खातों में हस्तक्षेप करके विदेशी ऋण चुकाएगा!!

भारत को विदेशी देशों से भारी कर्ज मिल रहा है और राष्ट्रीय खजाना तेज़ी से खाली होता जा रहा है। राज्यों के पास पैसे की कमी है और इस खर्च को पूरा करने का एकमात्र तरीका नागरिकों के बैंक खातों से सीधे पैसे निकालना है। निजी बैंकों ने पहले ही इस योजना से बाहर निकलने का ऐलान कर दिया है, लेकिन सरकारी बैंकों में कोई भी खाता अब दुरुपयोग से सुरक्षित नहीं है... (और पढ़ें)



चित्र: भारत के विदेश सचिव एक नए निजी बैंक के मालिक से हाथ मिलाते हुए

अभी रम्मी खेलें और 10,000 रुपये जीतें!!



### 3 विश्वसनीय तथ्य-जांच वेबसाइट्स खोजें। उनके नाम, यूआरएल और सत्यापन प्रक्रिया साझा करें:

---

---

---

---

याद रखें, गलत जानकारी की बड़ी कीमत चुकानी पड़ सकती है: यह लोगों की शारीरिक सुरक्षा, मानसिक स्वास्थ्य, और लोगों या समुदायों के बीच के रिश्तों और गरिमा पर असर डाल सकती है।

SUCS विधि बहुत मददगार है... लेकिन मुझे बहुत बेवकूफ और बुरामहसूस हो रहा है कि मैंने गलत जानकारी पर भरोसा किया और उसे फैलाया। मैं अपनी गलती भूल ही नहीं पा रहा...



कोई भी हमेशा गलत जानकारी को पकड़ने में सफल नहीं होता, तभी तो यह इतनी फैली हुई है! असली बात यह है कि हमें अपनी जानकारी जांचने की क्षमता को बेहतर बनाना है और जब सच्चाई पता चले, तो अपनी राय बदलने के लिए तैयार रहना चाहिए।



अमित भैया, मैं काफी परेशान हूँ! मुझे ढेर सारे मैसेज मिलते हैं। मैं इन सब की जांच करूंगा? इसमें तो पूरा दिन लग जाएगा!



हम्म... इंटरनेट पर हमें क्या महसूस होता है, इस पर ध्यान देना भी जरूरी है। मुझे भी कई बार ऑनलाइन बहुत ज्यादा चीजें देखकर घबराहट होती है, खासकर कुछ दिनों में...

यहां कुछ तरीके हैं, जिनसे मैं बिना किसी भ्रम के सूचना का जिम्मेदार उपभोक्ता बनने की कोशिश करता हूँ!

भरोसेमंद स्रोतों से समाचार पढ़ने के लिए एक तय समय तय करना।

याद रखना कि समय के साथ, सच को परखने की आदत अपने आप बेहतर हो जाएगी!

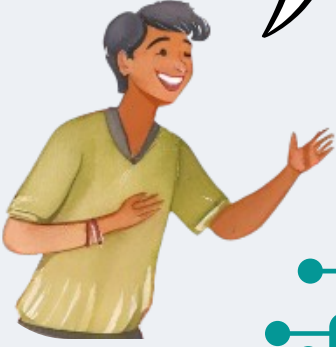
एक फैक्ट-चेकिंग साथी बनाना, जिससे मिलकर अभ्यास कर सकें और एक-दूसरे की गलतियां सुधार सकें!

किसी भी जानकारी को समझने और सोचने का समय लेना—लेकिन जब तक उसकी सटीकता को लेकर पक्का भरोसा न हो, उसे आगे न भेजना!



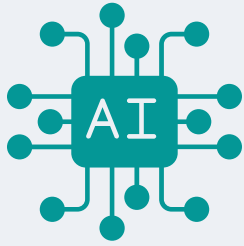
# ग़लत जानकारी और भ्रामक जानकारी कैसे फैलती हैं?

ग़लत जानकारी के तेज़ी से फैलने के पीछे के कारणों को समझना भी जरूरी है। यह समस्या हम सभी के लिए बड़ी है!



## क्लिकबेट और सनसनीखेज़ता

कंटेंट हमें क्लिक करने के लिए लुभाने के इरादे से बनाया जाता है – इसे अक्सर नाटकीय और बढ़ा-चढ़ाकर लिखा जाता है, ताकि हमें डर, उत्सुकता या जोश महसूस हो।



## डीपफेक और नकली बनाया कंटेंट

फोटो और वीडियो को असली दिखाने के लिए काफी एडिट किया जाता है – इससे लोग धोखा खा सकते हैं। कई बार यह ठगी का कारण बनता है या फिर लोगों के लुक्स को लेकर अवास्तविक उम्मीदें बना देता है।



## पुष्टि पूर्वाग्रह

हम उन खबरों पर जल्दी भरोसा कर लेते हैं जो हमारे विचारों से मेल खाती हैं। इसलिए, अगर कोई फेक न्यूज़ हमारी सोच से मिलती-जुलती हो, तो हम उसे बिना सोचे-समझे आगे भेज सकते हैं!



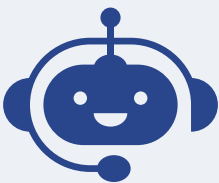
## बढ़ता ध्रुवीकरण

इंटरनेट पर बहसों बहुत गरम हो सकती हैं, क्योंकि अलग विचार रखने वालों के बीच दूरी बढ़ती जा रही है। इस माहौल में लोग ग़लत जानकारी बनाने या शेयर करने के लिए और भी प्रेरित महसूस कर सकते हैं।



## क्रेडिबिलिटी बायस (विश्वसनीयता का पूर्वाग्रह)

हम उन लोगों द्वारा दी गई जानकारी पर जल्दी भरोसा करते हैं, जिन पर हम भरोसा करते हैं – जैसे कि हमारे शिक्षक, रिश्तेदार या दोस्त। इससे परेशानी हो सकती है, क्योंकि हम खबर को नहीं, बल्कि व्यक्ति को जाँचते हैं!



## सोशल प्रूफिंग, बॉट्स और नकली प्रोफाइल

सोशल प्रूफिंग का मतलब है कि हम उस जानकारी पर जल्दी भरोसा करते हैं, जो बहुत लोकप्रिय लगती है। अब तो बॉट्स और फेक प्रोफाइल्स का इस्तेमाल किया जाता है, जिससे किसी पोस्ट को पॉपुलर दिखाया जाए – ताकि लोग उस पर यकीन कर लें!

## ऑनलाइन ज़िम्मेदारी से और सोच-समझकर व्यवहार करना



आपके हिसाब से हम गलत जानकारी से मुक्त इंटरनेट बनाने के लिए क्या कर सकते हैं?

---

---

---

अमित भैया, मुझे नहीं पता था कि गलत जानकारी की दुनिया इतनी पेचीदा है!



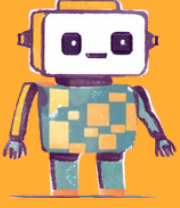
हाँ! मैंने भी इंटरनेट पर काफी कुछ पढ़ा और जानकारी की जांच करते हुए काफी नई चीज़ें सीखी...

यह तो कमाल है! अब ऐसा लग रहा है कि हम पहले से कम भटके हुए हैं और यह समझ पा रहे हैं कि हम क्या सोचते हैं, हमारी अपनी राय क्या है...



याद रखना, आलोचनात्मक सोच यानी क्रिटिकल थिंकिंग सिर्फ गलत चीज़ों से बचने के बारे में नहीं है। यह यह भी सीखना है कि तथ्यों और राय में फर्क कैसे करें, और किसी नतीजे पर सोच-समझकर पहुँचें... ग्लिच इसे और अच्छे से समझाएगा!





अक्सर, जो जानकारी आप ऑनलाइन इकट्ठा करते हैं, वह तथ्यों और राय का एक मिश्रण होती है। किसी भी जानकारी के दो हिस्सों के बीच अंतर करना आपकी आलोचनात्मक सोच की यात्रा में सहायक हो सकता है!

## तथ्य

बाहर बारिश हो रही है!

- सत्यापित किया जा सकता है
- अवलोकन या अध्ययन पर आधारित
- इस ग़लत साबित नहीं किया जा सकता

## राय

बारिश सब कुछ उदास कर देती है!

- एक ऐसा विश्वास या दृष्टिकोण, जिसे सत्यापित नहीं किया जा सकता, लेकिन उस पर चर्चा की जा सकती है।
- इसमें अच्छे या बुरे के बारे में पूर्वाग्रह और विचार हो सकते हैं।
- किसी तथ्य के बारे में किसी व्यक्ति की भावनाएं शेयर करना।



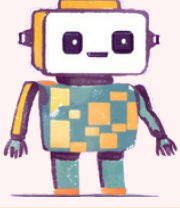
राय दुनिया को समझने का एक तरीका है और यह इस पर निर्भर करता है कि आप इसे कैसे देखते हैं। ये तथ्यों से समर्थित हो सकती हैं। राय पर बातचीत, बहस और खोजबीन की जा सकती है। लेकिन, अगर ये तथ्यों के खिलाफ होती हैं, तो इनकी वैधता खत्म हो जाती है।

तो यह पता करने के साथ कि स्रोत भरोसेमंद हैं और तथ्य सीधे हैं, हमें इस बात पर भी ध्यान देने की ज़रूरत है कि तथ्य और राय किस तरह आपस में जुड़े हुए हैं, है ना?

हाँ मुझे लगता है कि यह तुम्हें बहुत अच्छे से समझा दिया शुभम्! धन्यवाद, भैया!



## गतिविधि

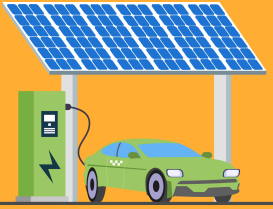


क्या आप नीचे दी गई जानकारी में तथ्यों को स्पष्ट कर सकते हैं और राय को उजागर कर सकते हैं? ऐसा करते समय, यह ध्यान में रखें कि क्या राय तथ्यों पर आधारित हैं और क्या आप उनसे सहमत हैं। आप इस विषय पर और भी पढ़ सकते हैं और देख सकते हैं कि क्या आपका विचार बदलता है!



स्ट्रॉबेरी एक ऐसा फल है जिसमें विटामिन सी होता है और यह सबसे स्वादिष्ट फल है।

कुतुब मीनार नई दिल्ली में है, लेकिन यह शहर के बाकी स्मारकों की तरह आकर्षक नहीं है।



इलेक्ट्रिक कारें गैस से चलने वाले वाहनों की तुलना में कम प्रदूषण करती हैं, जिससे ये पर्यावरण के प्रति जागरूक सभी लोगों के लिए एक बेहतरीन विकल्प बन जाती हैं।

अंतरिक्ष की खोज पर पैसा खर्च करना शायद बेकार लगे, लेकिन इससे अद्भुत तकनीकी विकास हुआ है।



फास्ट फूड में शुगर और फैट की मात्रा काफी ज्यादा होती है, यही वजह है कि यह दुनिया भर में मोटापे का एक बड़ा कारण बन गया है।

हर दिन पढ़ाई करने से ध्यान और शब्दावली में सुधार करने में मदद मिल सकती है, लेकिन कुछ लोग मानते हैं कि ऑडियोबुक भी उतनी ही प्रभावी होती हैं। मेरी राय में, अपने हाथों में एक असली किताब पकड़ने का अनुभव सबसे बेहतरीन होता है।



सोशल मीडिया एल्गोरिदम उस कंटेंट को प्राथमिकता देते हैं जो उपयोगकर्ताओं को जोड़कर रखती हैं, जिससे यह साफ होता है कि ये हमारे व्यवहार को प्रभावित करने के लिए बनाए गए हैं।

## एल्गोरिदम क्या होते हैं?



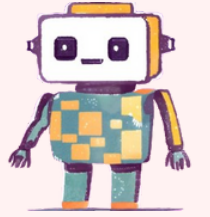
भारी बारिश के बाद एक गर्म और उमस भरा दिन था, और शुभम एक पेड़ के नीचे बैठकर अपनी आइसक्रीम का मजा ले रही थी। शुभम ने समाचार पढ़ने के लिए अपना फ़ोन निकाला, अब वह फ़र्जी खबरों को पहचानने में और भी तैयार महसूस कर रही थी लिकेन जैसे ही उसने स्क्रोल किया, उसे कुछ अजीब सा नजर आया।



हम्म, यह थोड़ा अजीब है। मुझे याद है कि कल बहुत तेज आंधी आई थी, लेकिन ऑनलाइन इसके बारे में कुछ भी नहीं मिल रहा है। मेरा न्यूज़फ़ीड तो कैफ़े की सिफ़ारिशों से भरा हुआ है!



ऐसा इसलिए होता है क्योंकि एल्गोरिदम आपकी गतिविधियों के आधार पर यह दिखाते हैं कि उन्हें क्या लगता है कि आपको पसंद आएगा। अगर आपने हाल ही में अपने आस-पास के कैफ़े के बारे में खोजा है, तो एल्गोरिदम आपको उस पर और जानकारी दिखाएगा!

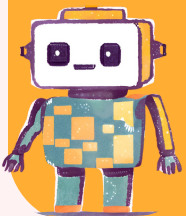


याद है न, हमने "डिजिटल दुनिया की पहली झलक" में इंटरनेट की तुलना रेलवे सिस्टम से की थी? एल्गोरिदम ठीक उसी तरह काम करते हैं जैसे ट्रेनों में स्टेशन मास्टर करते हैं! सोचिए, आप ट्रेन में हैं और हर बार जब आप किसी स्टेशन पर पहुँचते हैं, तो स्टेशन मास्टर देखता है कि आप कहाँ जा रहे हैं। अगर आप बार-बार उड़ीसा या बंगाल जैसी जगहों के लिए एक ही ट्रेन लेते हैं, तो स्टेशन मास्टर को ये लगने लगेगा कि आपको पूर्वी भारत के पर्यटन का मज़ा लेना पसंद है। अगली बार, वो आपको उन्हीं जगहों के लिए और ट्रेनें सुझाएंगे क्योंकि उन्हें लगता है कि आपको वहाँ जाना अच्छा लगता है।

इसी तरह, जब आप इंटरनेट का उपयोग करते हैं, तो एल्गोरिदम यह देखता है कि आप क्या कर रहे हैं - जैसे कि आप कौन से वीडियो देख रहे हैं, कौन से पेज पर जा रहे हैं या कौन सी चीज़ें खोज रहे हैं। अगर आप लगातार खाना पकाने से जुड़े वीडियो खोजते हैं, तो एल्गोरिदम यह मान लेता है कि आपको खाना बनाना पसंद है और आपको रेसिपी और खाने के टिप्स दिखाता है।



एल्गोरिदम आपकी ऑनलाइन गतिविधियों पर ध्यान देते हैं, जैसे कि आप क्या पसंद करते हैं, क्या टिप्पणी करते हैं या क्या साझा करते हैं। ये इंटरैक्शन आपकी रुचियों का संकेत देते हैं और प्लेटफ़ॉर्म को आपकी फ़ीड को बेहतर बनाने में मदद करते हैं। अगर आपको गेमिंग से जुड़ी पोस्ट पसंद हैं, तो एल्गोरिदम आपको और अधिक गेमिंग सामग्री, विज्ञापन और पेज दिखाएगा।

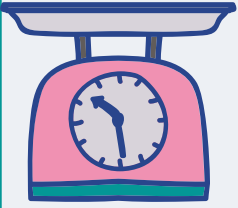
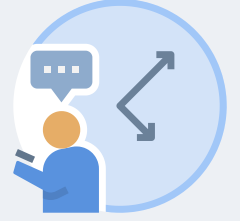


आप जिस तरह की सामग्री देखते हैं—चाहे वो वीडियो हो, लेख हो या तस्वीरें—इससे सिफ़ारिशें भी प्रभावित होती हैं। एल्गोरिदम उन फ़ॉर्मेट को प्राथमिकता देते हैं जिनसे आप सबसे ज़्यादा जुड़ते हैं।



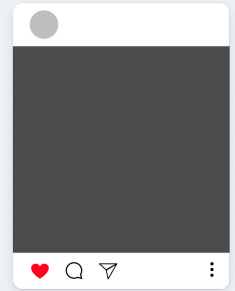
## एल्गोरिदम कैसे काम करते हैं?

आप जिस विषय पर जितना समय बिताते हैं, उससे एल्गोरिदम को ये समझ में आता है कि आपको कौन-सा विषय सबसे ज़्यादा पसंद है। जैसे-जैसे आप किसी खास विषय पर अधिक समय बिताते हैं, आपको उतनी ही ज़्यादा संबंधित पोस्ट दिखाई देंगी।



एल्गोरिदम का एक और अहम हिस्सा कंटेंट वेटिंग है, जो अलग-अलग तरह के पोस्ट और गतिविधियों को स्कोर देता है। प्लेटफ़ॉर्म पर सीधे अपलोड किए गए वीडियो को बाहरी साइटों के लिंक की तुलना में ज्यादा प्राथमिकता मिलती है। अच्छी क्वालिटी वाले स्रोतों से आने वाले लिंक को भी बढ़ावा दिया जाता है।

पोस्ट जब पुरानी हो जाती है, तो उनकी अहमियत कम हो जाती है। किसी पेज पर नई पोस्ट और हाल की बातचीत से उसकी सामग्री आपके फ़ीड में दिखने की संभावना बढ़ जाती है। अगर आपने किसी पेज के साथ कुछ समय से जुड़ाव नहीं रखा है, तो उसकी पोस्ट शायद कम बार दिखेंगी, चाहे वे नई ही क्यों न हों।



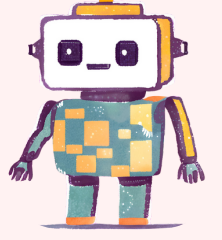
याद रखें! एल्गोरिदम उन चीज़ों को प्राथमिकता देते हैं जो ध्यान आकर्षित करती हैं, न कि जो सच में ज़रूरी हैं। वे अक्सर मशहूर कंटेंट को बढ़ावा देते हैं, जैसे कि आकर्षक शीर्षक या वायरल वीडियो, भले ही वो हमेशा सटीक या भरोसेमंद न हों। इसका मतलब है कि सबसे आकर्षक सामग्री ज़रूरी नहीं कि सबसे भरोसेमंद हो।

जबकि एल्गोरिदम आपके ऑनलाइन अनुभव को व्यक्तिगत बनाते हैं, वे आपको फ़िल्टर बबल में भी फंसा सकते हैं - एक ऐसा स्थान जहाँ आप केवल वही सामग्री देखते हैं जो आपकी मौजूदा रुचियों से मेल खाती है। इससे आप नए विचारों और दृष्टिकोणों नहीं जुड़ पाते हैं। इस बुलबुले से बाहर निकलने के लिए, अलग-अलग विषयों के बारे में पढ़ें और अलग-अलग तरह की कंटेंट देखें - क्या पता आपको कब क्या रोमांचक मिल जाए!



# एल्गोरिदम कैसे काम करते हैं?

एल्गोरिदम सिर्फ आपको कौन सा कंटेंट दिखेगा, यह तय नहीं करते, बल्कि यह भी तय करते हैं कि आपको कौन से विज्ञापन दिखेंगे। विज्ञापनदाता आपके ऑनलाइन व्यवहार का इस्तेमाल करते हैं, जैसे आपकी सर्च हिस्ट्री, क्लिक, और यहां तक कि आपकी लोकेशन, ताकि आपको ऐसे विज्ञापन दिखाए जा सकें जो खास तौर पर आपके लिए बनाए गए हों। आइए इसे स्टेप-बाय-स्टेप समझते हैं!



## विज्ञापन का लक्ष्य निर्धारण



एक बार जब विज्ञापनदाता आपका डेटा इकट्ठा कर लेते हैं, तो वे इससे इस बात को समझने की कोशिश करते हैं कि आपको क्या पसंद आ सकता है। विज्ञापनदाता उम्र, स्थान और पसंद - नापसंद जैसे डेटा का उपयोग करके विशिष्ट समूहों के लिए प्रासंगिक विज्ञापन दिखाते हैं।

## व्यक्ति की पसंद के हिसाब से लक्षित विज्ञापन



जो डेटा कंपनियों ने इकट्ठा किया होता है, उससे वे आपकी पसंद और आदतों का प्रोफाइल बनाते हैं। वे अंदाजा लगाते हैं कि आप किस तरह के विज्ञापन पर क्लिक करेंगे और आपको वही विज्ञापन दिखाते हैं जो उन्हें लगता है कि आपके लिए सबसे ज्यादा जरूरी हैं। इसीलिए, अगर आप ऑनलाइन नए फ़ोन देखते हैं, तो अचानक आपको फ़ोन कवर, चार्जर या ईयरफोन के विज्ञापन दिखने लगते हैं!

आप विज्ञापनदाताओं द्वारा इकट्ठा किए जाने वाले डेटा की मात्रा को कम करने और अपने ऑनलाइन अनुभव पर नियंत्रण पाने के लिए कुछ कदम उठा सकते हैं। आइए जानते हैं कि आप कैसे तय कर सकते हैं कि क्या शेयर करना है और क्या निजी रखना है!



गोपनीयता सेटिंग्स की जांच करें

लोकेशन ट्रैकिंग या व्यक्तिगत विज्ञापनों को बंद करने के लिए सेटिंग्स को बदलें।



कुकीज़ और कैश को साफ़ करें

विज्ञापन दिखाने वालों द्वारा इस्तेमाल किए जाने वाले डेटा को रीसेट करने के लिए समय-समय पर कुकीज़ को हटाते रहें।



एड ब्लॉकर्स का इस्तेमाल करें

विज्ञापनों को रोकें और ट्रैकर्स को आपका डेटा इकट्ठा करने से बचाएं।



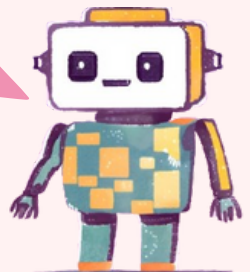
व्यक्तिगत विज्ञापनों को बंद करें

अपनी ऑनलाइन गतिविधियों पर आधारित विज्ञापनों को बंद करें आपको अभी भी विज्ञापन दिखेंगे, लेकिन वे आपकी ब्राउज़िंग हिस्ट्री के अनुसार नहीं होंगे।

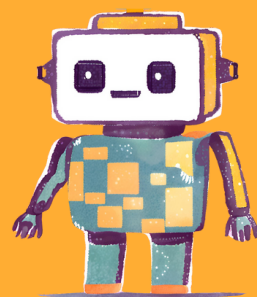
वाह, ये एल्गोरिदम तो कमाल का हैं, लेकिन थोड़ा डरावना भी! कोई आश्चर्य नहीं कि मेरे वीडियो सुझाव हमेशा बदलते रहते हैं। क्या ये विज्ञापन भी इसी से तय होते हैं? मैंने एक बार जूते खोजे, और अब मुझे बस वही दिख रहे हैं!



बिल्कुल सही! ये लक्षित विज्ञापन हैं, जो एल्गोरिदम के जरिए आपके डेटा का इस्तेमाल करने का एक और तरीका है!



तीन तरह के कंटेंट लिखिए, जो आप अपनी न्यूज़फ़ीड पर सबसे ज़्यादा देखते हैं। क्या ये वाकई आपके पसंदीदा विषय हैं, या आपको लगता है कि एल्गोरिदम ने आपके लिए एक तरह का 'बबल' बना दिया है? अपने विचार किसी दोस्त या क्लासमेट के साथ शेयर करें!



Blank white space for writing the first response.

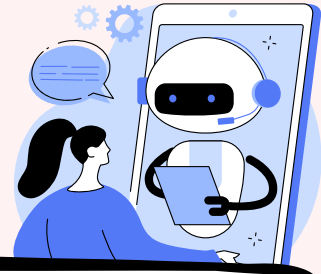
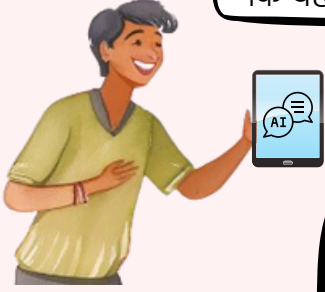
Blank white space for writing the second response.

Blank white space for writing the third response.



# आर्टिफिशल इंटेलिजेंस (AI) क्या है?

अरे दोस्तों! क्या तुमने इस AI चैटबॉट के बारे में सुना है? लगता है कि यह सब कुछ जानता है!



अरे हाँ! हम इसके बारे में तब एक साथ सीखे थे जब हम ऑनलाइन तकनीक और हमारे जीवन के बारे में पढ़ रहे थे। AI, यानी आर्टिफिशियल इंटेलिजेंस, उन कंप्यूटर सिस्टम्स को दर्शाता है जो मानव बुद्धि की नकल कर सकते हैं। जैसे, चैटबॉट सवालों के जवाब दे सकते हैं, सर्च इंजन वेबसाइट की सिफारिश कर सकते हैं, और इमेज पहचान उपकरण फोटोज में वस्तुओं को पहचान सकते हैं।

यह सच में बहुत दिलचस्प है! क्या तुम्हें समझ में आया कि यह कैसे चलता है?



हाँ! AI पैटर्न पहचानने और भविष्यवाणियाँ करने के लिए बहुत सारा डेटा प्रोसेस करता है। जैसे, अगर मैंने AI चैटबॉट से कोई सवाल पूछा, तो वह मेरे सवाल को समझेगा, उसका विश्लेषण करेगा, सबसे संबंधित जानकारी के लिए अपने डेटाबेस को खोजेगा और जवाब देगा - ये सब कुछ सेकंड में, एक सुपर-स्मार्ट सहायक की तरह!

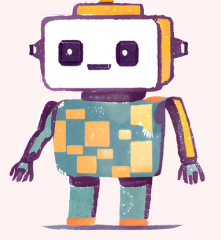


लेकिन ध्यान रखें, AI असल में इंसानों की तरह नहीं सोचता। यह बस अपने ट्रेनिंग डेटा का पालन करता है। यह बेहद मददगार हो सकता है, लेकिन इसकी ताकत और कमजोरियों को समझना जरूरी है। ग्लिच इसमें तुम्हारी मदद कर सकता है!



# एआई कैसे काम करता है?

आर्टिफिशियल इंटेलिजेंस एक ऐसा साथी है जो आपको कामों को जल्दी निपटाने, समस्याओं को सुलझाने और यहां तक कि सीखने को और भी मजेदार बनाने में मदद कर सकता है। हालांकि यह इंसान की तरह नहीं सोचता या महसूस नहीं करता, फिर भी AI आपके रोजमर्रा के जीवन के कई पहलुओं में काफी सहायक हो सकता है। चलिए देखते हैं कि AI आपकी मदद कैसे कर सकता है:



## डेटा तक जल्दी पहुंच

AI सेकंडों में भारी मात्रा में जानकारी का विश्लेषण कर सकता है। इसलिए रिसर्च और सीखने के लिए यह बहुत उपयोगी है।



## विचारों पर चर्चा

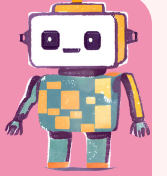
कभी नया आइडिया सोचते समय अटक जाते हो? AI रचनात्मक सुझाव देकर आपकी मदद कर सकता है। यह एक स्टीडी पार्टनर की तरह काम करता है!



## भाषा का अनुवाद

AI टूल भाषाओं की बाधा को तोड़ सकते हैं, जिससे आप दुनिया भर के लोगों से आसानी से बातचीत कर सकते हैं और दूसरी भाषाओं की सामग्री को समझ सकते हैं।

AI मददगार है, लेकिन इसमें कुछ कमियां भी हैं! जब भी AI का इस्तेमाल करें, इन बातों का ध्यान रखें:



## पक्षपात की समस्या

AI डेटा से सीखता है, और अगर इसका डेटा अधूरा या पक्षपाती हो, तो इसके जवाब भी गलत या एकतरफा हो सकते हैं।

## गलत जानकारी

AI कभी-कभी ऐसी बातें बना देता है जो सच नहीं होती! यह जवाब पैटर्न के आधार पर देता है, न कि असली तथ्यों पर।

## गोपनीयता को खतरा

कई AI टूल आपका डेटा इकट्ठा और विश्लेषण करते हैं ताकि वे बेहतर बन सकें। लेकिन इससे आपकी निजी जानकारी की सुरक्षा पर खतरा हो सकता है।



EXAMPLE

अगर किसी AI टूल को ज्यादातर पश्चिमी मीडिया पर ट्रेन किया जाता है, तो उसे भारत समेत दुनिया के दूसरे हिस्सों के सांस्कृतिक संदर्भों को समझने में मुश्किल हो सकती है।



EXAMPLE

अगर आप AI से किसी ऐतिहासिक व्यक्ति के बारे में पूछते हैं, तो यह कोई नकली उद्धरण या घटना बता सकता है, जो कभी हुई ही नहीं!

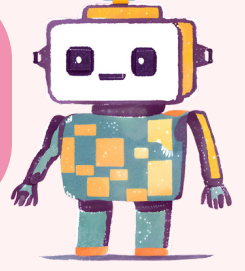


EXAMPLE

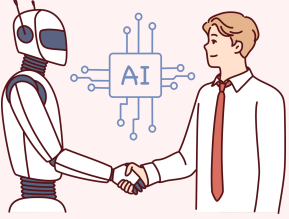
अगर कोई ऐप आपसे आपका स्थान मांगता है, तो यह जरूरी है कि आप सोचें कि उसे यह जानकारी क्यों चाहिए और क्या आप इसे साझा करने के लिए तैयार हैं।

## ग्लिच की एआई का इस्तेमाल करने की गाइड

ज़्यादा जानकारी से परेशान महसूस कर रहे हो? मैं समझ सकता हूँ! यह सब थोड़ा उलझाने वाला हो सकता है। लेकिन घबराओ मत, AI का सही इस्तेमाल करने के लिए ये आसान सुझाव अपनाओ:



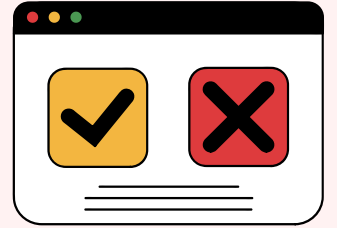
### AI के साथ सहयोग करें, उस पर निर्भर न रहें



AI मददगार हो सकता है, लेकिन यह आपकी खुद की सोच, रचनात्मकता और तर्क करने की क्षमता की जगह नहीं ले सकता। यह ब्रेनस्टॉर्मिंग या सुझाव लेने के लिए अच्छा है, लेकिन खुद से सोचना और नया बनाना सबसे ज़रूरी है!

### हमेशा तथ्य की जांच करें

AI हमेशा सही नहीं होता और कई बार गलत जानकारी दे सकता है। इसलिए जो भी जानकारी मिले, उसे भरोसेमंद स्रोतों – किताबों, विश्वसनीय वेबसाइटों, या अपने टीचर से पूछकर – ज़रूर जांचें।



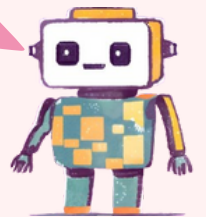
### इसकी सीमाओं को जानें

AI बहुत बुद्धिमान है, लेकिन यह इंसानों की तरह नहीं सोचता। यह लोगों की भावनाओं या सांस्कृतिक संदर्भों को उस तरह नहीं समझ पाता, जैसे लोग समझते हैं। इसे एक उपकरण की तरह देखिए, विशेषज्ञ की तरह नहीं!

तो मतलब, AI को एक शुरुआत के रूप में इस्तेमाल करना चाहिए, न कि अंतिम उत्तर मान लेना चाहिए?



बिल्कुल! इसे एक मददगार के रूप में समझें जो आपके काम को आसान बनाता है, लेकिन ये आपकी इंसानी सोच की जगह नहीं लेता।



### गतिविधि







अगर आपके पास इंटरनेट की पहुंच है

२ - २ की जोड़ी बनाएं। अब, आप में से एक AI टूल का इस्तेमाल कर सकता है और दूसरा पारंपरिक रिसर्च विधियों का उपयोग कर सकता है। अपनी पसंद के किसी भी विषय के बारे में सर्च करें। फिर, सटीकता, पूर्णता और विश्वसनीयता के लिए परिणामों की तुलना करें!

अगर आपके पास इंटरनेट की पहुंच नहीं है

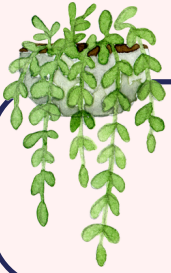
AI द्वारा बनाए गए उत्तर को फिर से लिखें। इसे और भी सटीक बनाने के लिए इसमें अधिक संदर्भ, उदाहरण और अपने विचार शामिल करें।

## चैप्टर रिकैप

-  ऑनलाइन जानकारी को आमतौर पर इन श्रेणियों में बांटा जा सकता है: विश्वसनीय जानकारी, व्यक्तिगत राय, गलत जानकारी (मिसइन्फॉर्मेशन), भ्रामक जानकारी (डिसइन्फॉर्मेशन) या फेक न्यूज़, और मनोरंजन और हास्य।
-  मिसइन्फॉर्मेशन आमतौर पर अनजाने में साझा की गई गलत या भ्रामक जानकारी होती है, जबकि डिसइन्फॉर्मेशन जानबूझकर लोगों को गुमराह करने के उद्देश्य से दी जाती है।
-  आप एक सरल विधि का उपयोग करके जानकारी की पुष्टि कर सकते हैं।
  - सोर्स (Source): क्या वेबसाइट विश्वसनीय और प्रसिद्ध है? क्या URL सुरक्षित है? क्या पेज का डिज़ाइन अच्छा है या पॉपअप से भरा हुआ है?
  - सर्वव्यापकता (Ubiquity): क्या जानकारी आम है और अन्य स्रोतों से सत्यापित की जा सकती है?
  - प्रसंग (Context): क्या नाम, तारीखें और स्थान सही हैं? क्या जानकारी पूरा है? क्या छवियाँ जानकारी से मेल खाती हैं?
  - दूसरी राय (Second Opinion): किसी विशेषज्ञ या तथ्य-जांचने वाली वेबसाइट जैसे ऑनलाइन संसाधन से दूसरी राय लें।
-  याद रखें: एल्गोरिदम उन चीज़ों को प्राथमिकता देते हैं जो ध्यान आकर्षित करती हैं, जरूरी नहीं कि वे सही या महत्वपूर्ण हों।
-  प्राइवैसी सेटिंग्स की समीक्षा करें, कुकीज़ और कैश हटाएं, ऐड ब्लॉकर का इस्तेमाल करें और व्यक्तिगत विज्ञापन बंद करें ताकि विज्ञापन एजेंसियों के साथ शेयर की जाने वाली जानकारी कम हो।
-  एआई बहुत सहायक हो सकता है, लेकिन इसमें नकली जानकारी फैलाने, पक्षपात करने और सेफ्टी चिंताओं को बढ़ाने की भी क्षमता है! हमेशा एआई द्वारा दी गई जानकारी की जांच करें, इसकी सीमाओं को समझें और इस पर पूरी तरह निर्भर होने की जगह इसे सहायक के रूप में इस्तेमाल करें।



# चैप्टर 5: गेम ओवर स्कैमर्स - ऑनलाइन खतरों को पहचानने और रोकें!



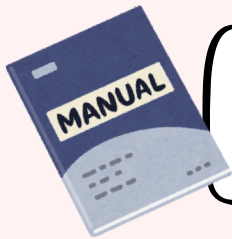
खिलखिलाती धूप से भरे एक सुनहरे दिन में जसप्रीत और नूर मिलकर, जसप्रीत के घर पर कुछ नए बीज लगा रहे हैं!



कल मैं जब शुभम के साथ था तो वह मुझे एल्गोरिदम, ए.आई. और कई और मजेदार के बारे में बता रही थी। उसने सिद्धार्थ और अमित भैया के साथ मिलकर इन चीजों के बारे में जानकारी इकट्ठा की थी। यह अनुभव वाकई दिलचस्प था, लेकिन इसने मुझे यह सोचने पर मजबूर कर दिया कि हमारे पास जानने के लिए कितना कुछ है...



इंटरनेट वाकई में दिलचस्प है, लेकिन जब हमें यह नहीं पता हो कि यह सुरक्षित है या नहीं, तो इसे इस्तेमाल करना थोड़ा मुश्किल हो जाता है।

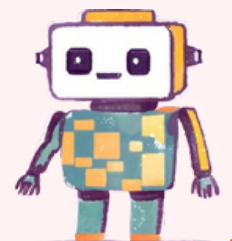


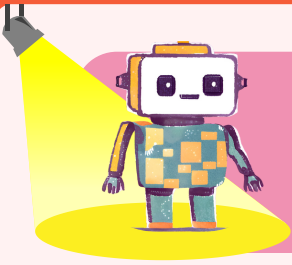
मुझे लगता है कि अगर हमारे पास इंटरनेट पर डरावनी और अनचाही बातचीत से निपटने के तरीके सीखने के लिए एक जगह हो, तो यह हम सभी के लिए बहुत फायदेमंद होगा। तुम इस बारे में क्या सोचती हो?



तुमने बिल्कुल सही कहा! मुझे लगता है कि ग्लिच इसमें हमारी सहायता कर सकता है!

जी हाँ! मैं बिल्कुल तुम्हारी सहायता कर सकता हूँ। चलिए, एक मजेदार सफ़र पर चलते हैं। ग्लिच की इंटरनेट सुरक्षा गाइड में आपका स्वागत है!





## आकाशगंगा के लिए ग्लिच की गाइड! इंटरनेट सुरक्षा

आपको आने वाले मैसेज, वीडियो, फोटो या अन्य संचार में आप खतरों की पहचान कैसे करते हैं? इसके लिए आपको लाल झंडों वाली सूची में दी गई बातों पर ध्यान देना चाहिए!

क्या उन्होंने आपकी व्यक्तिगत या संवेदनशील जानकारी (जैसे: उम्र, पता, फोन नंबर, स्कूल, बैंक खाता) मांगी है ?

क्या उन्होंने आपके निजी फोटो/वीडियो की मांग की, खासकर अनौपचारिक, मैत्रीपूर्ण बातचीत में?

क्या उन्होंने बहुत जल्दी आपके करीबी दोस्त बनने की कोशिश की, खासकर तारीफ या उपहार दे कर?

क्या उन्होंने आपसे अपनी बातचीत या कामों को दूसरों से छुपाने के लिए कहा है ?

क्या उन्होंने ऐसे अपमानजनक या दुखी करने वाले संदेश भेजे जिससे आपको असुरक्षित या दोषी महसूस हुआ?

क्या उन्होंने बड़े-बड़े वादे या प्रस्ताव किए (जैसे: लॉटरी, नौकरी का मौका)?



### इंटरनेट पर खतरों और असुरक्षित हालातों से बचने के लिए कुछ कदम!

- अक्षरों, संख्याओं और खास प्रतीकों का इस्तेमाल करके एक मजबूत पासवर्ड तैयार करें।
- 2-फैक्टर ऑथेंटिकेशन को सक्रिय करें
- सुनिश्चित करें कि आपकी प्रोफाइल की दृश्यता आपकी पसंद के अनुसार सेट की गई है - सार्वजनिक या निजी!
- सार्वजनिक मंचों पर अपना पूरा नाम, पता, फोन नंबर या स्कूल का नाम जैसी व्यक्तिगत जानकारी शेयर करने से बचें।
- संवेदनशील जानकारी (जैसे, बैंक विवरण) केवल एन्क्रिप्टेड प्लेटफॉर्म पर साझा करें।
- एंटीवायरस सॉफ्टवेयर इंस्टॉल करें और यह सुनिश्चित करें कि आपके डिवाइस का फ़ायरवॉल सक्रिय है।
- ईमेल या मैसेज में आने वाले अनजान लिंक पर क्लिक मत करें।
- असामान्य गतिविधियों की जांच के लिए अपने खातों की नियमित रूप से निगरानी करें।
- किसी भी ऐप को बहुत ज्यादा जानकारी इकठा करने न दें। अनावश्यक अनुमतियाँ अक्षम करें और उन ऐप्स से सावधान रहें जो अत्यधिक अनुमतियाँ मांगते हैं
- पॉप-अप, बेनर और वीडियो विज्ञापनों को रोकने और मैलवेयर से बचने के लिए एड ब्लॉकर्स का इस्तेमाल करें।
- सार्वजनिक वाई-फाई का इस्तेमाल करने से बचें और जब उपयोग में न हो तो अपना ब्लूटूथ बंद रखें।
- महत्वपूर्ण फाइलों या फोटो की कॉपियां बाहरी हार्ड ड्राइव पर सुरक्षित करें!

## केस स्टडी: ब्लू व्हेल चैलेंज



2016 में, "ब्लू व्हेल चैलेंज" नामक एक ऑनलाइन ट्रेंड सोशल मीडिया और पर्सनल मैसेज प्लेटफार्मों पर फैल गया। यह कोई साधारण खेल नहीं था-बल्कि यह ऑनलाइन धोखे का एक रूप था, जिसमें छात्रों को 50 दिनों तक खतरनाक कार्य करने के लिए बहकाया गया। इसे ऑनलाइन धमकियों और घोटालों की वास्तविक जीवन में नुकसान पहुँचाने की क्षमता के उदाहरण के रूप में देखा जाता है।

शुरुआत में, यह चैलेंज अजनबियों से निमंत्रण के रूप में फैलता गया-संदेश प्राप्त करने वालों से कहा गया कि उन्हें एक "विशेष गेम" के लिए चुना गया है, जिससे उनमें जिज्ञासा और उत्साह पैदा हुआ। जारी रखने के लिए, उन्हें एक अज्ञात "क्यूरेटर" या "गेम मास्टर" के निर्देशों का पालन करना पड़ता था, जो उन्हें प्रतिदिन कार्य सौंपता था। प्रारंभ में, कार्य सेफ लगते थे-एक व्हेल की तस्वीर बनाना, डरावनी फिल्म देखना या अजीब समय पर जागना। लेकिन धीरे-धीरे, प्रतिभागियों को खतरनाक जोखिम उठाने या अपने परिवार और दोस्तों से अलग होने के लिए कहा गया। प्रतिभागियों पर दबाव बनाने और उन्हें नियंत्रित करने के लिए इन् टेक्निक्स का इस्तेमाल किया गया था :

- प्राइवसी का उल्लंघन और ब्लैकमेल - इस खेल ने प्रतिभागियों को अपना पूरा नाम, पता या निजी तस्वीरें जैसी व्यक्तिगत जानकारी साझा करने के लिए धोखे में रखा। बाद में, इस जानकारी का उपयोग उन्हें धमकाने के लिए किया गया। संदेश जैसे "हमें पता है कि तुम कहाँ रहते हो" या "अगर तुमने गेम छोड़ा, तो हम तुम्हारे परिवार को नुकसान पहुँचाएँगे" भेजे गए ताकि प्रतिभागियों को चैलेंज में बनाए रखा जा सके। झूठे वादे भी किए गए।
- ऑनलाइन उत्पीड़न और धमकियाँ - जब किसी प्रतिभागी ने गेम छोड़ने की इच्छा जताई, तो उन्हें डरावने संदेश भेजे गए, जिनमें उन्हें कमजोर या असफल कहा गया। खिलाड़ियों को नकली ऑनलाइन समुदायों में भी शामिल किया गया, जहाँ उन्हें अपनी बहादुरी साबित करने के लिए दबाव महसूस हुआ।
- हैकिंग और ट्रैकिंग - कुछ खिलाड़ियों को लगा कि उनके डिवाइस हैक कर लिए गए हैं। उनकी स्क्रीन पर चेतावनी संदेश दिखाई देने लगे कि उन पर नज़र रखी जा रही है, जिससे उन्हें फँसा हुआ महसूस हुआ।

ब्लू व्हेल चैलेंज अब पहले की तरह व्यापक नहीं है, लेकिन नई ऑनलाइन धमकियाँ लगातार उभर रही हैं। जानकारी रखना, धोखे की रणनीतियों को पहचानना और मदद के लिए हाथ बढ़ाना आपको और दूसरों को डिजिटल दुनिया में सुरक्षित रख सकता है।

### Activity

ऐसे किसी खतरे या धोखाधड़ी, जैसे ब्लू व्हेल चैलेंज, का शिकार होने से बचने के लिए तीन ठोस उपाय बताइए।

श्रेष्ठ उत्तर

1. किसी भी अनजान व्यक्ति से किसी भी व्यक्तिगत जानकारी साझा करने से बचना।  
2. किसी भी अनजान व्यक्ति से किसी भी धमकी या खतरनाक संदेशों को न भेजना।  
3. किसी भी अनजान व्यक्ति से किसी भी धमकी या खतरनाक संदेशों को न भेजना।

## ऑनलाइन प्लेटफ़ॉर्म पर हानिकारक सामग्री की रिपोर्ट करना



यह एक बेहतरीन मौका है उन लोगों के लिए जो जल्दी खतरों से बचना सीखना चाहते हैं! बढ़िया काम, जसप्रीत और नूर!



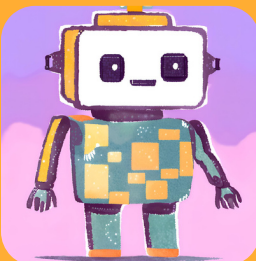
धन्यवाद अमित भैया!  
मेरे पास अभी भी एक सवाल है। मान लीजिए कि हम इन सभी बातों का ध्यानपूर्वक पालन करते हैं, लेकिन फिर भी हमें ऐसे संदेश या सामग्री मिलती है जो असुरक्षित लगती है। ऐसी स्थिति में हम क्या कर सकते हैं?



ओह, मैं कल इस पर एक वीडियो देख रहा था! मुझे पता चला कि ज्यादातर ऐप्स और प्लेटफ़ॉर्म में रिपोर्टिंग और ब्लॉकिंग की सुविधाएँ मौजूद हैं जिनका हम इस्तेमाल कर सकते हैं।



बिल्कुल सही कहा, जसप्रीत! ज्यादातर ऑनलाइन प्लेटफ़ॉर्म और मैसेजिंग ऐप में उत्पीड़न, धमकियाँ, प्रतिरूपण और गलत सूचना जैसी हानिकारक सामग्री की रिपोर्ट करने के लिए इन-बिल्ट टूल होते हैं। रिपोर्ट करना बहुत ज़रूरी है, क्योंकि इससे हम और हमारे आस-पास के लोग सुरक्षित रह सकते हैं।



**ग्लिच:** जब आप कंटेंट या मैसेजएस की रिपोर्ट करते हैं, तो इससे प्लेटफ़ॉर्म को अपराधियों के खिलाफ़ कदम उठाने, खुद को और दूसरों को ऑनलाइन दुर्व्यवहार से बचाने और हानिकारक सामग्री को फैलने से रोकने में मदद मिलती है। रिपोर्टिंग का मतलब यह नहीं है कि हमेशा तुरंत कार्रवाई होगी, लेकिन अगर कई उपयोगकर्ताओं द्वारा एक सामग्री को रिपोर्ट किया जाता है तो प्लेटफ़ॉर्म द्वारा उस समस्या को सुलझाने की संभावना बढ़ जाती है।

## ऑनलाइन प्लेटफॉर्म पर हानिकारक सामग्री की रिपोर्ट कैसे करें और उसे कैसे रोके

ज्यादातर प्लेटफॉर्म पर, हानिकारक सामग्री या चैट की रिपोर्ट करना काफी आसान है। ऐसा करने के लिए आप कुछ सरल स्टेप्स का पालन कर सकते हैं। याद रखें कि ये स्टेप्स आपके द्वारा इस्तेमाल किए जा रहे प्लेटफॉर्म के अनुसार अलग भी हो सकते हैं। यदि आपको इनके बारे में कोई संदेह हो तो किसी भरोसेमंद वयस्क या दोस्त से पूछ लें।

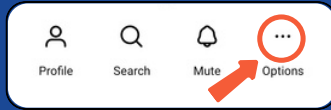
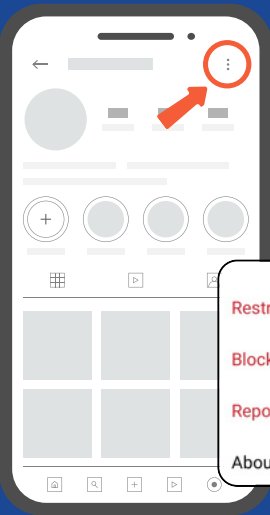
1

रिपोर्ट करने से पहले चैट या कंटेंट का स्क्रीनशॉट लेना न भूलें, ताकि अगर आगे कुछ करना पड़े तो आपके पास सबूत मौजूद हो। अपने फोन पर स्क्रीनशॉट लेने के लिए पावर/होम बटन और वॉल्यूम बटन को एक साथ दबाएं (यह आपके फ़ोन के मॉडल के हिसाब से अलग भी हो सकता है)।

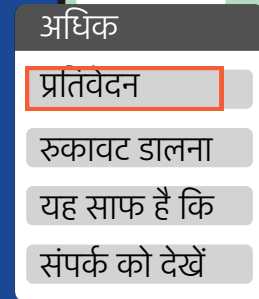
मेनू विकल्प पर क्लिक करें और मेनू में "रिपोर्ट", "अधिक" या "सहायता प्राप्त करें" का चयन करें।

हानिकारक सामग्री के अनुसार सबसे उपयुक्त ऑप्शन का चयन करें (जैसे, उत्पीड़न, गलत जानकारी, प्रतिरूपण, अभद्र भाषा आदि)।

2



कई मैसेजिंग प्लेटफॉर्म पर सिर्फ रिपोर्ट करने के बजाय "ब्लॉक और रिपोर्ट" करने का ऑप्शन भी होता है। इससे वो व्यक्ति आपसे फिर संपर्क नहीं कर पाएगा।



अगर आप किसी फर्जी अकाउंट या प्रोफाइल की रिपोर्ट करना चाहते हैं (शायद कोई आपके या आपके किसी जानने वाले का नाम लेकर काम कर रहा हो), तो आप मेनू या अधिक जानकारी बटन को इसी तरह ढूँढ सकते हैं, और "प्रोफाइल की रिपोर्ट करें" पर क्लिक कर सकते हैं।

अगर आप किसी खास चैट या संदेश की रिपोर्ट करना चाहते हैं, तो आपको उस संदेश को दबाकर रखना होगा या रिपोर्ट विकल्प खोजने के लिए "बातचीत सेटिंग्स" चेक करनी होंगी (यह "अधिक" सेटिंग के तहत हो सकता है)।

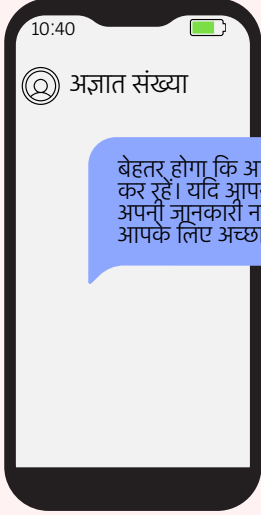
3

रिपोर्ट दाखिल करें और दिए गए निर्देशों का पालन करें।

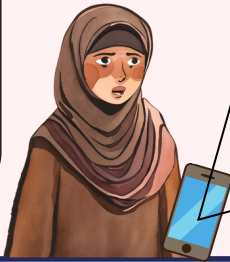
जब आप किसी कंटेंट या चैट की रिपोर्ट करते हैं, तो प्लेटफॉर्म उसे हटाने, अकाउंट को प्रतिबंधित करने या चेतावनी देने का निर्णय ले सकता है। कुछ प्लेटफॉर्म आपकी रिपोर्ट पर अपडेट प्रदान करेंगे, जबकि अन्य ऐसा नहीं भी कर सकते हैं।

## साइबर अपराधों की रिपोर्टिंग करना

नूर को अपने फोन पर एक धमकी भरा संदेश मिलता है। वह डर जाती है और उस संदेश को प्लेटफ़ॉर्म पर रिपोर्ट कर देती है और उसे ब्लॉक कर देती है! लेकिन 5 मिनट बाद, उसे एक अलग प्लेटफ़ॉर्म के ज़रिए उसी प्रोफ़ाइल से एक और संदेश मिलता है।



बेहतर होगा कि आप संभल कर रहें। यदि आपने मुझे अपनी जानकारी नहीं दी, तो आपके लिए अच्छा नहीं होगा!



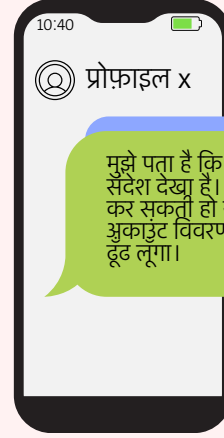
अधिक

रिपोर्ट करें

ब्लॉक करें

चैट डिलीट करें

संपर्क को देखें



मुझे पता है कि तुमने मेरा आखिरी संदेश देखा है। तू मुझे इग्नोर नहीं कर सकती हो नूर! मुझे अभी अपना अकाउंट विवरण भेज दो, वरना मैं तुम्हें हूड लूंगा।



मैंने प्लेटफ़ॉर्म पर अकाउंट की रिपोर्ट की, लेकिन वे अभी भी मुझे संदेश भेज रहे हैं! मुझे सुरक्षित महसूस नहीं हो रहा है... मैं और क्या कर सकती हूँ?



अगर यह एक गंभीर मामला है, तो मुझे लगता है कि हमें इसकी शिकायत साइबर क्राइम सेल को करनी चाहिए। मैंने सुना है कि वे ऑनलाइन धमकियों, उत्पीड़न और डिजिटल धोखाधड़ी से निपटते हैं। सही कहा न, अमित भैया?

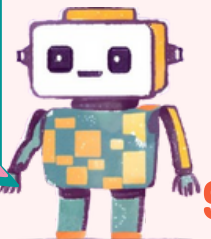


हाँ जसप्रीत! ग्लिच, क्या तुम हमें कुछ ज़रूरी हेल्पलाइनों के बारे में बता सकते हैं?



बिल्कुल अमित भैया!

आप साइबर अपराध की रिपोर्ट [cybercrime.gov.in](http://cybercrime.gov.in) पर कर सकते हैं या तुरंत मदद के लिए 1930 पर कॉल कर सकते हैं। और अगर खतरा लिंग आधारित है, तो आप राष्ट्रीय महिला आयोग (NCW) हेल्पलाइन 7827-170-170 पर भी संपर्क कर सकते हैं। वे ऑनलाइन उत्पीड़न, ब्लैकमेल और दुर्यवहार के मामलों में सहायता करते हैं।



## साइबर अपराध की शिकायत करने के लिए सरकारी हेल्पलाइन

अगर आप या आपका कोई जानने वाला ऑनलाइन दुर्व्यवहार, धमकी, ब्लैकमेल या उत्पीड़न का सामना कर रहा है, तो इसकी रिपोर्ट दर्ज कराएं।



साइबर अपराध विभाग (राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल)

- वेबसाइट: [cybercrime.gov.in](http://cybercrime.gov.in)
- हेल्पलाइन: 1930
- साइबरस्टॉकिंग, ऑनलाइन धमकियाँ, पहचान की चोरी, हैकिंग वगैरह की रिपोर्ट करता है।



राष्ट्रीय महिला आयोग (एनसीडब्ल्यू)

- वेबसाइट: [ncw.nic.in](http://ncw.nic.in)
- हेल्पलाइन: 7827-170-170
- महिलाओं को हानि पहुंचाने वाले अपराधों पर करवाई करता है, जिसमें ऑनलाइन उत्पीड़न और दुर्व्यवहार भी शामिल हैं।



स्थानीय थाने

- फ़ोन नंबर: 100
- साइबर अपराध के मामलों की शिकायत आप अपने नजदीकी पुलिस स्टेशन में भी कर सकते हैं।
- आप एफआईआर भी दर्ज करवा सकते हैं।



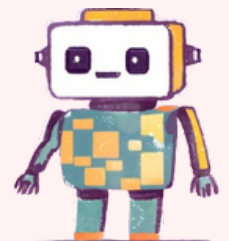
चाइल्डलाइन इंडिया (बच्चों की ऑनलाइन सुरक्षा के लिए)

- वेबसाइट: [childlineindia.org](http://childlineindia.org)
- हेल्पलाइन: 1098
- बच्चों के खिलाफ ऑनलाइन धमकियों, साइबर धमकी और अन्य डिजिटल अपराधों का सामना करना।

यह सूची मेरे लिए काफी फायदेमंद है, धन्यवाद ग्लिच! अगर मैं इनमें से किसी एक नंबर पर कॉल करती हूँ या उनकी वेबसाइट पर जाती हूँ तो मैं शिकायत कैसे दर्ज करूँ? मुझे कौन सी जानकारी चाहिए होगी?



कुछ बातें हैं जो ध्यान में रखनी चाहिए। चलो देखते हैं!



1

स्टेप 1: साक्ष्य इकट्ठा करें

- धमकियों या संदेशों का स्क्रीनशॉट लें या URL को सेव करें।
- उनके टाइमस्टैम्प और वह नंबर या आईडी लिख लें जिससे आपको संदेश मिला है।

http://



2

स्टेप 2: शिकायत को दर्ज करें

- cybercrime.gov.in पर जाएं और रिपोर्ट जमा करें। अगर आप चाहें तो इसे गुमनाम भी रख सकते हैं।
- अगर आप रिपोर्ट दर्ज कराने या हेल्पलाइन पर कॉल करने में सक्षम नहीं हैं, तो आप अपने नजदीकी पुलिस स्टेशन में जाकर एफआईआर भी दर्ज करा सकते हैं।



स्टेप 3: फॉलो-अप

अपनी शिकायत की स्थिति पर ध्यान दें और जरूरत पड़ने पर गैर सरकारी संगठनों, कानूनी विशेषज्ञों या सहायता संगठनों से मदद लें।

3

गतिविधि: चलो देखते हैं कि आपको क्या याद है!

1. भारत में साइबर अपराध की रिपोर्ट करते समय अधिकारियों के लिए किस तरह का साक्ष्य सबसे ज्यादा मददगार होता है?

- क) अपराध से जुड़े किसी भी दस्तावेज़ की फिजिकल कॉपी
- ख) स्क्रीनशॉट, ईमेल बातचीत और धोखाधड़ी से संबंधित सामग्री की डिजिटल कॉपी
- ग) फोन कॉल के दौरान घटना का मौखिक विवरण
- घ) पीड़ित के रिश्तेदारों से अपराध की पुष्टि करने वाला हस्ताक्षरित हलफनामा

2. सत्य या असत्य: भारत में साइबर अपराध की रिपोर्ट करने के लिए पुलिस थाने जाना जरूरी है।

- क) सच
- ख) झूठ

3. भारत में साइबर अपराधों की रिपोर्ट करने के लिए हेल्पलाइन नंबर क्या है?

- क) 100
- ख) 112
- ग) 1930
- घ) 1098

## गतिविधि, चल रही है. ..

4. आपका दोस्त आपको बताता है कि एक अनजान शख्स उन्हें साइबर-स्टॉक कर रहा है। वह उन्हें लगातार मैसेज करता रहता है और उनकी ऑनलाइन गतिविधियों पर नजर रखता है। उन्हें सबसे पहले क्या करना चाहिए?

क) ऐप पर स्टॉकर को ब्लॉक करें और रिपोर्ट करें।

ख) स्टॉकर को जवाब दें और उनसे कहें कि वे ऐसा करना बंद करें।

ग) सोशल मीडिया अकाउंट को तुरंत डिएक्टिवेट करें और लोकेशन बंद कर दें।

घ) स्थिति को नजरअंदाज करें ताकि स्टॉकर की रुचि खत्म हो जाए।

5. निम्नलिखित में से कौन सी गतिविधि आपकी साइबर सुरक्षा के लिए सबसे बड़ा खतरा बन सकती है?

क) कई महत्वपूर्ण खातों के लिए एक ही मजबूत पासवर्ड का इस्तेमाल करना

ख) सार्वजनिक वाई-फाई से जुड़ना और संवेदनशील खातों में लॉग इन करना

ग) महत्वपूर्ण खातों पर 2-फैक्टर ऑथेंटिकेशन (2FA) चालू करना

घ) ब्लूटूथ और स्थान सेवाओं को केवल जरूरत पड़ने पर ही चालू रखना

6. किसी वयस्क से मदद लेने का सही समय कब है?

क) क्या आप किसी ऑनलाइन संदेश के चलते असहज या असुरक्षित महसूस कर रहे हैं?

ख) क्या आपको अपनी बातचीत और गतिविधियों को दूसरों से छिपाने के लिए कहा गया है?

ग) क्या आपको किसी नए ऑनलाइन दोस्त से बड़ा नकद पुरस्कार मिलने का प्रस्ताव मिला है?

घ) उपरोक्त सभी

अगर नूर शिकायत करती है, तो उसके बाद क्या होगा?



लेकिन मैं यह कैसे पता करूँ कि कोई चीज़ अपराध की श्रेणी में आती है या नहीं ?



रिपोर्ट दर्ज करने के बाद, साइबर पुलिस जांच कर सकती है, अपराधी का पता लगा सकती है और कानूनी कार्रवाई कर सकती है। अगर तुम्हें तत्काल खतरा महसूस हो रहा है, तो अपने नज़दीकी पुलिस स्टेशन को सूचित करना सबसे अच्छा रहेगा।



अच्छा सवाल है। ऑनलाइन धमकियाँ हमेशा डरावनी होती हैं और नीचे दिए गए व्यवहार के शामिल होने पर वह अपराध की श्रेणी में आती है

हिंसा या नुकसान की चेतावनियाँ

यौन उत्पीड़न या पीछा करना

बिना अनुमति के निजी तस्वीरें साझा करना

प्रतिरूपण, धोखाधड़ी, या पहचान की चोरी

# हमारी सुरक्षा के लिए कानून

इंटरनेट एक ताकतवर जगह है जहां हम एक-दूसरे से जुड़ते हैं, सीखते हैं और चीजें साझा करते हैं। असली दुनिया की तरह, इंटरनेट पर भी हमारी सुरक्षा सुनिश्चित करने के लिए कुछ कानून हैं। अगर कोई आपसे चोरी करता है, आपको धमकाता है या आपकी प्राइवैसी का उल्लंघन करता है, तो उसे भारतीय कानून के तहत सजा मिल सकती है। चाहे अपराध ऑनलाइन ही क्यों न हुआ हो!

## सूचना प्रौद्योगिकी (आई. टी.) अधिनियम, 2000

आईटी अधिनियम भारत का मुख्य साइबर कानून है, जो लोगों को हैकिंग, पहचान की चोरी, ऑनलाइन उत्पीड़न और गोपनीयता के उल्लंघन से सुरक्षित रखता है।



### डेटा की चोरी (धारा 43)

अगर कोई आपकी डिवाइस को हैक कर लेता है या आपकी अनुमति के बिना आपका डेटा चुरा लेता है, तो उस पर ₹1 करोड़ तक का जुर्माना लगाया जा सकता है।

### पहचान की चोरी (धारा 66सी)

किसी और के नाम या तस्वीर का इस्तेमाल करके नकली सोशल मीडिया प्रोफाइल बनाना अवैध है, जिसके लिए 3 साल तक की जेल और 1 लाख रुपये का जुर्माना हो सकता है।



### गोपनीयता का उल्लंघन (धारा 66ई)

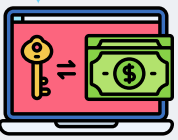
बिना अनुमति के निजी तस्वीरें या वीडियो शेयर करना एक अपराध है, जिसके लिए 3 साल तक की जेल और 2 लाख रुपये का जुर्माना हो सकता है।

### हैकिंग (धारा 66)

किसी के कंप्यूटर या सोशल मीडिया को बिना अनुमति से एक्सेस करना, नुकसान पहुंचाना या लॉक करना 3 साल तक की जेल और 5 लाख रुपये के जुर्माने की सजा का कारण बन सकता है।



## भारतीय दंड संहिता (आईपीसी), 1860



### साइबर एक्सटॉर्शन (साइबर जबरन वसूली) (धारा 384)

अगर कोई आपको पैसे न देने पर आपकी निजी चैट या फोटो लीक करने की धमकी देता है, तो उसे साइबर जबरन वसूली कानून के तहत सजा मिल सकती है।

### ऑनलाइन पीछा और उत्पीड़न (धारा 354डी)

ब्लॉक करने के बाद भी किसी को बार-बार संदेश भेजना, उसका पीछा करना या ऑनलाइन परेशान करना अवैध है।



### गुमनाम धमकियाँ (धारा 507)

अगर कोई शख्स अपनी पहचान छुपाकर, नकली सोशल मीडिया अकाउंट, गुमनाम ईमेल या मैसेजिंग ऐप के जरिए धमकी देता है, तो उसे इस कानून के तहत सजा मिल सकती है।

# हमारी सुरक्षा के लिए कानून

## उपभोक्ता सुरक्षा अधिनियम, 2019

यह कानून उपभोक्ताओं को ऑनलाइन धोखाधड़ी, घोटालों और अनुचित व्यापार प्रथाओं से सुरक्षा प्रदान करता है। अगर कोई ऑनलाइन शॉपिंग साइट खराब उत्पाद को वापस करने से मना करती है, तो आप इस अधिनियम के तहत शिकायत कर सकते हैं।

### गतिविधि: कानूनों का मिलान करें!

नीचे पाँच अलग-अलग ऑनलाइन अपराध और उनके खिलाफ बनाए गए पाँच कानून दिए गए हैं। हर अपराध को सही कानून से जोड़ें!

बिना अनुमति के निजी फोटो लीक कर दी गई।	हैकिंग
कोई आपके कंप्यूटर को हैक करके फाइलें मिटा देता है।	उपभोक्ता सुरक्षा कानून
कोई कंपनी आपको खराब उत्पाद के लिए पैसे वापस करने से मना कर देती है।	चोरी की पहचान करना
एक अनजान शख्स फर्जी अकाउंट से बार-बार धमकियाँ दे रहा है।	निजता का हनन
कोई शख्स आपके नाम से फर्जी प्रोफाइल बना देता है।	गुमनाम धमकियाँ

मुझे नहीं पता था कि ऑनलाइन दुनिया में हमारी सुरक्षा के लिए इतने सारे कानून हैं! लेकिन अगर मुझे नहीं पता कि किसी स्थिति में कौन सा कानून लागू होता है, तो फिर क्या होगा?

कोई बात नहीं! सबसे जरूरी यह है कि जब कुछ गलत लगे, तो उसे पहचानें और किसी भरोसेमंद वयस्क या अधिकारियों को बताएं। तुम्हें हर कानून के बारे में जानने की जरूरत नहीं है, लेकिन अपने अधिकारों के प्रति जागरूक रहना फायदेमंद होता है!



यह बात तो सही है। तो, अगर कोई मुझे ऑनलाइन परेशान कर रहा है, तो मुझे धारा 354D याद रखने की जरूरत नहीं है - मुझे बस इसकी रिपोर्ट करनी है और मदद लेनी है?

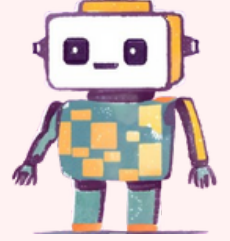


बिल्कुल सही! और अगर तुम्हें कभी भी शक हो, तो तुम हमेशा इन नियमों को देख सकते हो या मदद मांग सकते हो। सहायता हमेशा उपलब्ध है!

# ऑनलाइन मदद लेना और दूसरों की मदद करना

इंटरनेट कनेक्ट होने, सीखने और मस्ती करने के लिए एक शानदार जगह हो सकती है - लेकिन जब चीजें गलत हो जाती हैं तो क्या होता है? अगर आप कभी असुरक्षित, परेशान महसूस करते हैं या आपको बस किसी से बात करने की ज़रूरत महसूस होती है, तो मदद सिर्फ एक कॉल दूर है।

चाहे आप ऑनलाइन उत्पीड़न, बदमाशी, संकट या मानसिक स्वास्थ्य से जुड़ी समस्याओं का सामना कर रहे हों, आपकी मदद के लिए विश्वसनीय हेल्पलाइन, परामर्शदाता और संगठन मौजूद हैं। यह जानना कि मदद कहाँ से प्राप्त करें और दूसरों की सहायता कैसे करें, ऑनलाइन सुरक्षित रहने का एक ज़रूरी हिस्सा है।



चाइल्डलाइन इंडिया फाउंडेशन

ध्यान केंद्रित: डराना, शोषण, भावनात्मक सहायता  
1098 (टोल-फ्री)



एनसीपीसीआर (राष्ट्रीय बाल अधिकार संरक्षण आयोग)

ध्यान केंद्रित: बच्चों के अधिकारों का उल्लंघन, धमकी, उत्पीड़न  
1800-121-2830 (टोल-फ्री)



महिला हेल्पलाइन डब्ल्यूएचएल (निर्भया फंड, महिला और बाल विकास मंत्रालय)

ध्यान केंद्रित: ऑनलाइन उत्पीड़न, सुरक्षा की चिंताएं  
181 (टोल-फ्री)



एनसीडब्ल्यू (राष्ट्रीय महिला आयोग)

ध्यान केंद्रित: ऑनलाइन यौन उत्पीड़न, महिलाओं के अधिकार  
011-26942369 / 26944754



AASRA हेल्पलाइन

ध्यान केंद्रित: आत्महत्या रोकने, भावनात्मक संकट में मदद  
91-9820466726



पुकारना

ध्यान केंद्रित: निजी भावनात्मक परामर्श, मानसिक स्वास्थ्य सहायता

022-25521111 (सोमवार से शनिवार, सुबह 8 बजे से रात 10 बजे तक)



मानस फाउंडेशन

ध्यान केंद्रित: मानसिक स्वास्थ्य सहायता, संकट और बदमाशी के लिए परामर्श +91 97117 00069



बचपन बचाओ आंदोलन

ध्यान केंद्रित: लापता बच्चे, बाल श्रम, तस्करी, शोषण  
1800-102-7222 (टोल-फ्री, 24/7)

# भावनात्मक प्राथमिक चिकित्सा: संकट के समय खुद को शांत करना



ये हेल्पलाइन सच में बहुत मददगार हैं! लेकिन नूर, अगर मैं उसी समय घबराने लगूं तो फिर क्या होगा? क्या तुम्हारे पास मुझे शांत करने का कोई तरीका है? मुझे लगता है कि मैं चीजों को ठीक करने की कोशिश में इतना खो जाता हूँ कि मैं भूल जाता हूँ कि मैं कैसा महसूस कर रहा हूँ।

मैं समझ गई कि तुम क्या कहना चाह रहे हो! जब ऑनलाइन कुछ तनावपूर्ण होता है, जैसे लड़ाई या किसी से बहस, तो बिना सोचे-समझे प्रतिक्रिया देना आसान होता है। लेकिन एक पल रुक कर अपनी भावनाओं को संभालना वाकई मददगार हो सकता है। चलो, मैं तुम्हें कुछ आसान तरीके बताती हूँ जो शायद मददगार हों!



## स्वयं को शांत करने के आसान तरीके: जब भी आप तनाव में हों, तो इन तकनीकों को अपनाएं!

5-4-3-2-1 ग्राउंडिंग एक्सरसाइज

अपने विचारों को डायरी में लिखें।

दृश्य देखना और गहरी साँस लेना

अपने चारों ओर देखें। पहचानें:

- 5 चीजें जो आप देख सकते हैं।
- 4 चीजें जो आप छू सकते हैं
- 3 बातें जो आप सुन सकते हैं।
- 2 ऐसी चीजें जिनकी आप खुशबू ले सकते हैं
- 1 वह चीज जिसका आप स्वाद ले सकें

जो कुछ हुआ, उससे आपको कैसा महसूस हुआ और इस बारे में आगे आप क्या कदम उठा सकते हैं, ये सब के बारे में लिखिए।

अपने विचारों को कागज पर लिखने से आपको अपनी भावनाओं को समझने, स्पष्टता पाने और प्रतिक्रिया देने से पहले सोच-समझकर निर्णय लेने में मदद मिलती है।

सबसे पहले, अपनी आँखें बंद करें और एक शांत, सुरक्षित जगह की कल्पना करें - एक ऐसी जगह जहाँ आप पूरी तरह से आरामदायक महसूस करते हैं। यह एक शांत पार्क, एक आरामदायक कमरा या शांत पहाड़ हो सकता है। आपकी सुरक्षित जगह वह है जहाँ आप सुरक्षित, सहज, और नियंत्रित महसूस करते हैं।

अब, एक धीमी और गहरी साँस लें, उस जगह के दृश्य, आवाज़ और भावनाओं पर ध्यान दें। अपने आपको इस पल का पूरा अनुभव करने दें।





## गतिविधि: अपनी शांति की योजना बनाएं

अगली बार जब आप तनाव में हों, तो आप कौनसी शांत करने वाली गतिविधि करना चाहेंगे?

आपका सुरक्षित स्थान (चाहे वो असली हो या काल्पनिक) कहाँ है, जहाँ आप आराम महसूस करते हैं?

कोई ऐसा वाक्य लिखें जिसे आप मुश्किल समय में खुद से कह सकें। (उदाहरण: "मैं मजबूत हूँ। यह क्षण भी गुजर जाएगा।")

वाह! यह सच में बहुत मददगार है - धन्यवाद नूर! मैं ज़रूर अपने लिए भी एक प्लान बनाऊंगा।



क्या तुम्हारे पास ऐसे किसी दोस्त की मदद करने के लिए कोई सुझाव है जो ऐसी ही स्थिति में हो सकता है? उन्हें सिर्फ रिपोर्ट करने या तुरंत कार्रवाई करने के लिए कहना कभी-कभी असंवेदनशील लगता है, और मैं जानना चाहता हूँ कि उनकी सबसे अच्छी तरह से कैसे मदद की जाए!

तुम बिलकुल सही हो - एक दोस्त ऑनलाइन उत्पीड़न या नकारात्मकता के चलते भावनात्मक और मानसिक रूप से परेशान हो सकता है, लेकिन हो सकता है कि वे मदद मांगने में हिचकिचा रहे हों। यह भी हो सकता है कि उन्होंने पहले ही किसी अपराध की रिपोर्ट कर दी हो, फिर भी वे बेचैन महसूस कर रहे हों। मुझे लगता है कि अपने दोस्तों का समर्थन करने के बारे में जानना वाकई ज़रूरी है और इससे बहुत फ़र्क पड़ सकता है।

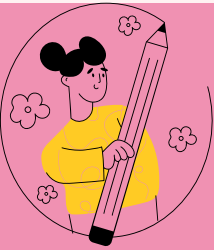


# सामाजिक प्राथमिक चिकित्सा: संकट में फंसे दोस्त के लिए एक बेहतरीन सहायक तंत्र कैसे बनाएं



**सक्रिय रूप से सुनना** - जब कोई दोस्त अपने संघर्षों के बारे में बात कर रहा हो, तो तुरंत समाधान देने की कोशिश मत करो। इसके बजाय, उन्हें बिना किसी रुकावट के अपनी बात कहने का मौका दो। उन्हें अपनी भावनाओं को खुलकर व्यक्त करने दो और उनकी भावनाओं को स्वीकार करो। कभी-कभी, यह जानना कि कोई बिना जज करे आपकी बात सुन रहा है, सलाह से ज्यादा सुकून देने वाला हो सकता है।

**चेक इन करें और फॉलो अप करें** - "हे, क्या हाल है? आप कैसे हैं?" जैसा एक छोटा संदेश भी बहुत बड़ा फर्क डाल सकता है। भले ही वे कहें कि सब ठीक है, फॉलो अप करना और बाद में चेक इन करना ये दिखाता है कि आप सच में उनकी परवाह करते हैं। अगर वे ऑनलाइन तनाव, हिंसा या उत्पीड़न का सामना कर रहे हैं, तो अनौपचारिक बातचीत उन्हें बिना किसी दबाव के समर्थन महसूस करने में मदद कर सकती है।



**सीमाएँ तय करने में मदद करें** - अगर वे ऑनलाइन उत्पीड़न या नकारात्मकता का सामना कर रहे हैं, तो उन्हें याद दिलाएं कि उनके पास अपने स्पेस पर नियंत्रण है। उन्हें हानिकारक यूजर्स को ब्लॉक करने और रिपोर्ट करने के साथ-साथ अपनी प्राइवैसी सेटिंग्स को एडजस्ट करने के लिए प्रेरित करें। अगर उन्हें यह करने में संदेह है, तो उनकी इस प्रक्रिया में मदद करने की पेशकश करें।

आप उन्हें इंटरनेट सुरक्षा, गोपनीयता सेटिंग और ऑनलाइन समय प्रबंधन के बारे में बेहतर तरीके से समझने के लिए इस गाइडबुक को भी साझा कर सकते हैं। सही जानकारी के साथ, आप और आपके आस-पास के लोग एक सुरक्षित और स्वस्थ डिजिटल अनुभव बना सकते हैं।







## गतिविधि: आपकी व्यक्तिगत सुरक्षा की सूची



तैयार रहना आपके ऑनलाइन तनावपूर्ण या असुरक्षित हालात से निपटने में काफी मदद कर सकता है। यह सुनिश्चित करने के लिए कि आपके पास सही उपकरण और सहायता प्रणाली है, नीचे दी गई चेकलिस्ट को पूरा करें।

- ऊपर दी गई हेल्पलाइन में से कम से कम एक का चयन करें और उसे अपने फोन में सेव कर लें या किसी ऐसी जगह लिख लें जहाँ आप आसानी से उसे देख सकें। संकट के समय, यह जानना कि मदद कहाँ से जल्दी मिल सकती है, बहुत फायदेमंद हो सकता है।
- ऐसे दो लोगों के बारे में सोचें जिनसे आप मदद मांग सकते हैं - ये कोई परिवार का सदस्य, शिक्षक, या करीबी दोस्त हो सकते हैं। उनके नाम लिख लें ताकि मुश्किल समय में आपको याद रहे।
- गहरी साँस लेना, जर्नलिंग या ग्राउंडिंग एक्सरसाइज में से कोई एक शांत करने वाली तकनीक चुनें। जब भी आप अभिभूत महसूस करें, इसका उपयोग करके अभ्यास करें।
- संकट में फंसे दोस्त की मदद करने के लिए एक सामाजिक प्राथमिक चिकित्सा योजना का अभ्यास करें।

## चैप्टर रिकैप

-  ऐसे मैसेज से सावधान रहें जो आपकी निजी जानकारी मांगते हैं, गिफ्ट या वादे का लालच देते हैं, तस्वीरें मांगते हैं, या बातचीत को गुप्त रखने के लिए कहते हैं !
-  सभी मैसेजिंग और सोशल मीडिया प्लेटफॉर्म पर रिपोर्ट और ब्लॉक करने का ऑप्शन होता है - अगर कभी संदेह हो, तो इसका इस्तेमाल ज़रूर करें !
-  अगर ऑनलाइन रिपोर्ट या ब्लॉक करने से बात न बने, तो साइबर क्राइम सेल (फोन: 1930 या [cybercrime.gov.in](http://cybercrime.gov.in)) या अपने नज़दीकी पुलिस स्टेशन (100 नंबर) पर शिकायत करें।
-  ऑनलाइन खतरों में ये चीज़ें शामिल हो सकती हैं - धमकी देना, परेशान करना, किसी की निजी तस्वीरें बिना इजाज़त शेयर करना, किसी की नकल करना, धोखा देना या पहचान चुराना।
-  आईटी एक्ट २०००, िप्स १८६० और कंस्यूमर प्रोटेक्शन एक्ट २०१९ जैसे कई कानून हैं जो डिजिटल दुनिया में हमारे अधिकारों की रक्षा करते हैं।
-  सबसे ज़रूरी बात - आप अकेले नहीं हैं! आपके परिवार और दोस्त आपके साथ हैं, ज़रूरत पड़ने पर उनकी मदद लें।



# चैप्टर 6: क्लिक, स्क्रोल, आराम! डिजिटल दुनिया में सुकून

इंटरनेट एक शानदार जगह है जो कुछ सीखने, दूसरों से जुड़ने और खुद को अभिव्यक्त करने के अवसरों से भरपूर है। जीवन के अन्य पहलुओं और स्थानों की तरह, इंटरनेट भी कुछ अनूठी चुनौतियाँ प्रस्तुत करता है। इन चुनौतियों को पहचानना, स्वस्थ ऑनलाइन आदतें बनाना और सुरक्षित और नियंत्रित रहते हुए अपनी डिजिटल दुनिया का अधिकतम लाभ उठाना महत्वपूर्ण है।



मीरा देर रात तक अपने फोन का इस्तेमाल करती रहती है। वह अपने दोस्तों के रोमांचक अपडेट और मजेदार वीडियो देखती है। लेकिन इसके साथ उसे कई नकारात्मक खबरें और टिप्पणियाँ भी दिखती हैं जिससे उसे बेचैनी होती है। अगली सुबह वह थका हुआ महसूस करती है।

मैं स्क्रॉल करते हुए भी इतना थका हुआ क्यों महसूस कर रही हूँ? क्या यह कंटेंट की वजह से हो रहा है या फिर... हर चीज़ बहुत अधिक हो गयी है?



लगता है तुम बहुत देर से स्क्रॉल कर रही हो। कभी-कभी, ऑनलाइन रहना एक रोलरकोस्टर की तरह महसूस हो सकता है - एक पल में आपका मनोरंजन होता है, दूसरे ही पल आप ऐसी चीज़ देखते हैं जो आप पर बोझ डालती है। एक पल रुक कर यह जांचना कि तुम्हारी ऑनलाइन गतिविधि तुम्हें कैसा महसूस करा रही है, शायद सही रहेगा

हाँ, यह बड़ा अजीब है। कुछ चीज़ें मुझे हंसाती हैं, लेकिन फिर कुछ परेशान करने वाली चीज़ें दिख जाती हैं, और अचानक मुझे बुरा लगता है।



- इस बारे में सोचें कि आप आखिरी बार कब ऑनलाइन थे—सिर्फ़ सोशल मीडिया पर ही नहीं, बल्कि किसी ऐप या वेबसाइट का इस्तेमाल करते हुए। चाहे वह समाचार हो, शॉपिंग हो या बैंकिंग ऐप, हम इंटरनेट के साथ कैसे इंटरैक्ट करते हैं, इसका असर हमारी भावनाओं पर पड़ सकता है।
- क्या समाचार ब्राउज़ करते समय आपको जानकारी प्राप्त होने के साथ-साथ चिंता भी हुई?
- क्या आपको खरीदारी से क्षणिक रोमांच तो मिला, लेकिन बाद में पछतावा हुआ?
- दिन के किस समय आपने ऐप या वेबसाइट का उपयोग किया?

इन तत्वों का विश्लेषण करने से आपको उन भावनाओं के बारे में जानकारी प्राप्त करने में मदद मिल सकती है जो आपके इंटरनेट उपयोग को संचालित करती हैं। साथ ही आप यह भी समझ सकते हैं कि इंटरनेट आपके मूड को कैसे प्रभावित करता है।



## गतिविधि

इंटरनेट वेल-बीइंग स्कोरकार्ड  
निर्देश:

- निम्नलिखित 10 प्रश्नों के उत्तर ईमानदारी से दें।
- यदि आप ऐसा अक्सर करते हैं तो प्रत्येक कथन के लिए स्वयं को 1 अंक दें।

आपकी सोशल मीडिया आदतें

- मैं सुबह उठते ही सबसे पहले अपना फोन (सोशल मीडिया, समाचार, शॉपिंग एप्स) चेक करता हूँ।
- मुझे स्क्रॉल करना बंद करना कठिन लगता है, तब भी जब मेरे पास करने के लिए अन्य काम हों।
- मैं समाचार पढ़ने या ऑनलाइन अपडेट देखने के बाद तनावग्रस्त या चिंतित महसूस करती हूँ।
- मैं अपने जीवन की तुलना ऑनलाइन जो कुछ भी देखता हूँ उससे करता हूँ - चाहे वह लोग हों, रुझान हों या जीवनशैलियाँ हों।
- मैं तब भी ऑनलाइन खरीदारी करती हूँ जब मुझे किसी चीज़ की जरूरत नहीं होती, ताकि मैं अच्छा महसूस कर सकूँ।
- मैं इंटरनेट का उपयोग तब करता हूँ जब मैं उदास, ऊबा हुआ या परेशान महसूस करता हूँ।
- मैं देर रात तक जागती रही, अपनी नींद त्यागती रही, ताकि ब्राउज़िंग या स्क्रॉलिंग जारी रख सकूँ।
- मैं संदेशों, टिप्पणियों या सूचनाओं का तुरंत जवाब देने के लिए दबाव महसूस करता हूँ।
- ऑनलाइन होने के कारण मैं वास्तविक जीवन की गतिविधियों (शौक, स्कूल का काम, परिवार के साथ समय बिताना) से दूर रहने लगी हूँ।
- मुझे तब बहुत दुख होता है जब मेरी पोस्ट को पर्याप्त लाइक, कमेंट या प्रतिक्रिया नहीं मिलती।

स्कोर विश्लेषण

0-3 अंक - बढ़िया! आपका सोशल मीडिया के साथ अच्छा रिश्ता है।

4-6 अंक - संतुलित! आप ठीक चल रहे हैं, लेकिन आपको कुछ आदतों के प्रति सचेत रहना चाहिए।

7-10 अंक - आपका सोशल मीडिया उपयोग आपके स्वास्थ्य को प्रभावित कर सकता है। रीसेट करने का समय आ गया है!

चिंतन एवं कार्रवाई

- क्या आपके स्कोर के बारे में किसी बात ने आपको आश्चर्यचकित किया?
- अपनी डिजिटल खुशहाली को बेहतर बनाने के लिए आप कौन सा एक छोटा बदलाव कर सकते हैं?

सोचें कि आपने कौन से कथनों को चुना और क्यों। क्या वे किसी खास प्लैटफ़ॉर्म, ऐप या मूड से संबंधित थे? कभी-कभी, कुछ खास ट्रिगर्स—जैसे देर रात तक बोरियत या तनाव—हमें इंटरनेट का अत्यधिक उपयोग करने के लिए प्रेरित करते हैं। इस अध्याय में आगे, हम स्वस्थ विकल्प चुनने के तरीकों के बारे में जानेंगे।

सिद्धार्थ ने दो साल पहले डिजिटल चैंपियंस प्रोग्राम पूरा किया, और वह अपने दोस्तों के लिए ऑनलाइन सुरक्षा के मुद्दों पर एक मार्गदर्शक बन गया। धोखाधड़ी को पहचानने से लेकर गोपनीयता नियंत्रण स्थापित करने तक, वह जानता है कि डिजिटल दुनिया में जिम्मेदारी से कैसे काम किया जाए। लेकिन हाल ही में, उसे उसके माता-पिता असहज लग रहे थे - बढ़ते डिजिटल अपराधों की खबरों के चलते वे काफी चिंतित थे। एक शाम, खाने के दौरान, सिद्धार्थ ने अंततः पूछा,



माँ, पापा, क्या आपको कभी इस बात की चिंता होती है कि मैं ऑनलाइन कितना समय बिताता हूँ?

हम तुम पर भरोसा करते हैं और जानते हैं कि तुम इन सभी वर्षों में इंटरनेट का उपयोग सावधानी से कर रहे हो। लेकिन हाल ही में, हम समाचारों में कई चिंताजनक रुझान देख रहे हैं। हम तुम्हें डराना नहीं चाहते, लेकिन हम यह सुनिश्चित करना चाहते हैं कि तुम इंटरनेट पर सुरक्षित और सतर्क रहो- ठीक वैसे ही जैसे हम भीड़-भाड़ वाली जगह पर करते हैं। हम पिछले दिनों मीरा के माता-पिता से भी इस बारे में बात कर रहे थे।



तो क्या मुझे इंटरनेट का इस्तेमाल बिल्कुल नहीं करना चाहिए? या फिर सिर्फ तब इस्तेमाल करना चाहिए जब मैं आपके आस-पास हूँ?

बिल्कुल नहीं— इंटरनेट इस्तेमाल न करना समाधान नहीं है। आओ हम मिलकर कुछ सरल, व्यावहारिक नियम तय करें जो तुम्हारी स्वतंत्रता का सम्मान करते हुए तुम्हें इंटरनेट पर सुरक्षित रखें। हम कुछ सीमाएँ तय कर सकते हैं और देख सकते हैं कि तुम कैसा महसूस करते हो।



## हमें हमेशा इंटरनेट का कम उपयोग करने के लिए क्यों कहा जाता है?

हममें से कई लोगों के मन में यह सवाल है—“वयस्क लोग क्यों कहते रहते हैं, ‘फ़ोन नीचे रखो?’” यह सिर्फ स्क्रीन टाइम के बारे में नहीं है; यह स्क्रीन के पीछे क्या हो रहा है, इसके बारे में है। एक पल को सोशल मीडिया को एक महासागर के रूप में सोचें—विशाल, रोमांचक और नए अवसरों से भरा हुआ। कुछ क्षेत्रों में क्रिस्टल-क्लियर पानी होता है जहाँ आप सीख सकते हैं, जुड़ सकते हैं और आगे बढ़ सकते हैं। लेकिन कभी-कभी कोई व्यक्ति डूम-स्कॉलिंग की छिपी धाराओं में खो सकता है। इंटरनेट आपको व्यस्त रखने के लिए बनाया गया है—सामग्री और सूचनाएँ सभी आपके लिए विशेष रूप से संशोधित और वैयक्तिकृत की जाती हैं। लेकिन हम इस बात के प्रति सचेत रह सकते हैं कि हम ऑनलाइन कितना समय बिताते हैं और हम किससे जुड़ रहे हैं। लक्ष्य पूरी तरह से डिस्कनेक्ट होना नहीं है, बल्कि नियंत्रण में रहना है—इंटरनेट का उपयोग ऐसे तरीकों से करना जो हमें विचलित करने के बजाय हमारे जीवन में मूल्य जोड़ें और फायदा पहुंचाएँ।

## चेकलिस्ट: जब सोशल मीडिया बहुत ज़्यादा लगने लगे

सिद्धार्थ की तरह, हम सभी को अपने इंटरनेट उपयोग के बारे में कुछ बुनियादी दिशा-निर्देश स्थापित करने चाहिए। इसमें पहला कदम यह पहचानना है कि क्या सुरक्षित लगता है और क्या नहीं। नीचे आत्म-मूल्यांकन के कुछ तरीके दिए गए हैं। यदि आप खुद को निम्नलिखित में से किसी भी भावना का अनुभव करते हुए पाते हैं, तो यह समय है थोड़ा रुककर सोचने का।

चिंतित या असुरक्षित महसूस करना

शारीरिक संकेत: छाती में भारीपन, बेचैनी, या मूड में उतार-चढ़ाव।

निरंतर तुलना करना

आप स्वयं को दूसरों की उपलब्धियों के आधार पर खुद को मापते हुए पाते हैं।

बातचीत से नाराज़ या दुखी होना

बातचीत या टिप्पणियाँ आपको पहले से अधिक तनावग्रस्त कर देती हैं।

नींद खोना

आप देर रात तक स्क्रॉल करते रहते हैं या अपना फीड रिफ्रेश करते रहते हैं।

अलगाव महसूस होना

आप ज्यादा अकेला महसूस करते हैं, भले ही आप इंटरनेट से क्यों न "जुड़े" हों।

लाइक और कमेंट के बारे में अधिक सोचना

आप अपने दिमाग में इंटरनेट पर मिली प्रतिक्रियाओं को बार-बार दोहराते रहते हैं।

भावनात्मक रूप से थकान

ऑनलाइन रहने के बाद आप थका हुआ या कमजोर महसूस करते हैं।



याद रखें, आपके फ़ोन को भी रिचार्ज करने की ज़रूरत होती है - आपको भी! अगर सोशल मीडिया आपको खुश करने के बजाय निराश कर रहा है, तो आइए रीसेट करने और बेहतर महसूस करने के तरीके खोजें।



हर किसी की ऑनलाइन यात्रा अलग-अलग होती है - एक व्यक्ति के लिए जो काम करता है वह दूसरे के लिए काम नहीं कर सकता है। सोशल मीडिया कनेक्ट होने और सीखने के लिए बहुत बढ़िया है, लेकिन हमें अपने डिजिटल जीवन को अपने असली जीवन के साथ संतुलित करने की आवश्यकता है। वास्तविक जीवन के अनुभव हमारे विकास, कनेक्शन और समग्र कल्याण के लिए आवश्यक हैं।



मेरे अनुभव और खोज के आधार पर, यहां कुछ ऐसी चीजें दी गई हैं जो सोशल मीडिया के साथ एक स्वस्थ संबंध बनाने में मदद करती हैं।

## सोशल मीडिया के साथ स्वस्थ संबंध बनाना

1. सकारात्मक और प्रेरणादायक कंटेंट फॉलो करें।
2. उत्साहवर्धक वार्तालापों में भाग लेकर डिजिटल दयालुता का अभ्यास करें।
3. आप इंटरनेट से जुड़ी ऐप्स पर कितना समय व्यतीत करते हैं, इसके लिए दैनिक सीमा निर्धारित करें।
4. उन ऐप्स के लिए नोटिफिकेशन बंद करें, जिन पर आपको तुरंत ध्यान देने की ज़रूरत नहीं है।
5. जब आपको ब्रेक या ध्यान केंद्रित करने के लिए समय की आवश्यकता हो तो 'डू नॉट डिस्टर्ब' सुविधा का उपयोग करें।
6. देर रात तक स्क्रॉल करने से बचने के लिए सोशल मीडिया के उपयोग पर प्रतिबंध लगाएं।
7. "वन-नाइट रूल" का प्रयोग करें, जिसमें आप कुछ भी पोस्ट करने से पहले एक दिन प्रतीक्षा करते हैं।
8. जब दूसरों की हरकतें सोशल मीडिया को तनावपूर्ण बना देती हैं
  - नकारात्मक सामग्री के साथ इंजोमेंट सीमित करें।
  - यदि आवश्यक हो तो म्यूट करें, अनफॉलो करें या ब्लॉक करें।
  - किसी से बात करें - मित्र, माता-पिता, शिक्षक।
9. सकारात्मकता के लिए सोशल मीडिया का उपयोग करें।



## खुशी मेनू

याद रखें, आपकी स्क्रीन के बाहर एक पूरी दुनिया है! जब इंटरनेट बहुत भारी लगे, तो एक कदम पीछे हटें—आपका जीवन सिर्फ पिक्सल और नोटिफिकेशन तक सीमित नहीं है। सांस लेने के लिए ताज़ी हवा है, मिलने के लिए असली लोग हैं, और स्क्रॉल से परे कई अनुभव आपका इंतज़ार कर रहे हैं। आपके सबसे अच्छे पल सिर्फ ऑनलाइन नहीं होते। यहाँ एक हैप्पीनेस मेनू है — सेरोटोनिन बढ़ाने वाली गतिविधियों की एक सूची जिसे आप अपने मूड को बेहतर बनाने के लिए चुन सकते हैं और खुद को याद दिला सकते हैं कि खुशी ऑफ़लाइन भी मौजूद है!

- |  |   |
|--|---|
| <input type="radio"/> अपने पसंदीदा गाने पर नृत्य करें              | <input type="radio"/> दयालुता भरा कोई कार्य करें          |
| <input type="radio"/> प्रकृति में सैर के लिए जाएं                  | <input type="radio"/> सूर्यास्त देखें                     |
| <input type="radio"/> किसी मित्र को बातचीत के लिए बुलाएं           | <input type="radio"/> अपनी पसंदीदा जगह पर जाएं            |
| <input type="radio"/> अपने विचारों को जर्नल में लिखें              | <input type="radio"/> लक्ष्य सूची बनाएं                   |
| <input type="radio"/> कोई खेल खेलें                                | <input type="radio"/> आरामदायक स्नान करें                 |
| <input type="radio"/> पेंटिंग करें, ड्रिलिंग करें या कलाकृति बनाएं | <input type="radio"/> कोई पुस्तक या कविता पढ़ना           |
| <input type="radio"/> उत्साहवर्धक संगीत सुनें                      | <input type="radio"/> अपने भविष्य के लिए पत्र लिखें       |
| <input type="radio"/> गहरी साँस लेना या ध्यान                      | <input type="radio"/> अपने कमरे की साफ़ सफाई करें         |
| <input type="radio"/> कुछ पकाना या पकाना                           | <input type="radio"/> किसी उद्देश्य के लिए स्वयंसेवक बनें |

ऊपर दी गई सूचीबद्ध गतिविधियाँ केवल कुछ उदाहरण हैं। मुख्य बात यह है कि अपनी जरूरतों को सुनें और पहचानें कि आपके मूड और मानसिक स्वास्थ्य के लिए सबसे अच्छा क्या है। खुद से पूछकर शुरुआत करें:

- क्या चीज़ मुझे अच्छा और ऊर्जावान महसूस कराती है?
- जब मैं बहुत परेशान हो जाता हूँ तो मुझे शांत होने में क्या मदद करता है?
- कौन सी गतिविधियाँ मुझे खुशी देती हैं या मुझे संतुष्टि का अहसास कराती हैं?



एक बार जब आप इन गतिविधियों की पहचान कर लें, तो उन्हें अपनी दिनचर्या में शामिल कर लें। समय के साथ, ये आदतें आपको अपने ऑनलाइन और ऑफलाइन जीवन के बीच संतुलन बनाने में मदद करेंगी, जिससे यह सुनिश्चित होगा कि आप सोशल मीडिया को अपने ऊपर नियंत्रण करने देने के बजाय नियंत्रण में रहें।

अपने मानसिक स्वास्थ्य का ख्याल रखने का मतलब है यह पहचानना कि उतार-चढ़ाव जीवन का एक स्वाभाविक हिस्सा हैं - जिसमें ऑनलाइन जीवन भी शामिल है। सोशल मीडिया सीखने, जुड़ने और प्रेरणा के लिए एक जगह हो सकती है, लेकिन यह आत्म-संदेह या तुलना के क्षण भी ला सकती है। जब आप लगातार हाइलाइट रीलों को स्क्रॉल करते हैं तो यह महसूस करना आसान है कि आप पीछे रह गए हैं - लेकिन याद रखें, आप जो ऑनलाइन देखते हैं वह अक्सर वास्तविकता का एक ध्यान से तैयार किया गया संस्करण होता है, न कि पूरी सच्चाई।

गलत सूचना और भ्रामक सूचनाओं के बारे में हमने जो अध्ययन किया है, उस पर विचार करें—जैसे झूठी खबरें फैल सकती हैं, वैसे ही अवास्तविक डिजिटल व्यक्तित्व भी फैल सकते हैं। लोग अक्सर अपने जीवन के केवल सबसे अच्छे हिस्सों को ही साझा करते हैं, जिससे चीजें वास्तविकता से कहीं अधिक परिपूर्ण लगती हैं। लेकिन हर पोस्ट के पीछे एक वास्तविक व्यक्ति होता है, जिसके संघर्ष, असुरक्षा और चुनौतियाँ आपकी तरह ही होती हैं।

अपने आप को यह याद दिलाना महत्वपूर्ण है कि आप जो देखते हैं वह हमेशा पूरी कहानी नहीं होती। अपनी वास्तविकता की तुलना किसी की हाइलाइट रील से करने के बजाय, अपना ध्यान उस पर केंद्रित करें जो आपको वास्तव में खुशी और संतुष्टि देता है।



आपकी खुशी आपके पोस्ट पर आने वाले लाइक और कमेंट या आपके फॉलोअर्स की संख्या से कहीं अधिक महत्वपूर्ण है!



समय के साथ, मैंने सीखा है कि इंटरनेट का उपयोग करने के तरीके के बारे में सोचना महत्वपूर्ण है। मैं सोचता था कि मुझे अपडेट रहने के लिए हर समय ऑनलाइन रहना होगा, लेकिन मुझे एहसास हुआ कि यह सही नहीं है। अब, मैं अपने ऑनलाइन समय के बारे में अधिक जागरूक होने और सीमाएँ निर्धारित करने की कोशिश करता हूँ ताकि मैं इसमें न फँस जाऊँ। मैं उन चीजों के लिए भी समय निर्धारित करता हूँ जो मुझे रिचार्ज करने में मदद करती हैं, जैसे दोस्तों और परिवार के साथ समय बिताना, प्रकृति में रहना, या बस अपने लिए कुछ समय निकालना। यह हमेशा आसान नहीं होता है, लेकिन मैंने पाया है कि लंबे समय में यह इसके लायक है।



## रिकैप : क्लिक, स्कॉल, सांस ले

ऑनलाइन रहते हुए अपनी भावनाओं पर ध्यान दें।



इंटरनेट मज़ेदार हो सकता है, लेकिन ये भी देखें कि इससे आपको कैसा महसूस होता है। अगर ऑनलाइन रहने के बाद आप थके हुए, उदास, या परेशान महसूस करें, तो थोड़ी देर का ब्रेक लें।

ऑनलाइन और ऑफलाइन जीवन में संतुलन बनाए रखें।



बहुत ज़्यादा ऑनलाइन रहने से आपकी नींद, मूड और ध्यान पर असर पड़ सकता है। अपने शौक पूरे करें, दोस्तों के साथ समय बिताएं, और असली दुनिया का भी आनंद लें।

अपनी भलाई के लिए सीमाएँ तय करें।



छोटे कदम, जैसे गैरज़रूरी नोटिफिकेशन बंद करना, सोशल मीडिया के लिए समय सीमा तय करना और देर रात स्कॉलिंग से बचना, आपकी डिजिटल आदतों पर नियंत्रण बनाए रखने में मदद कर सकते हैं।

याद रखें, सोशल मीडिया पूरी सच्चाई नहीं है।



जो आप ऑनलाइन देखते हैं, वो सिर्फ़ बेहतरीन पल होते हैं - पूरी ज़िंदगी नहीं। दूसरों से तुलना करने की बजाय अपनी खुशियों और लक्ष्य पर ध्यान दें।

अगर कुछ गड़बड़ लगे, तो बात करें।



अगर कभी इंटरनेट आपको असहज या असुरक्षित लगे, तो किसी भरोसेमंद इंसान से बात करें। आप अकेले नहीं हैं - हमेशा मदद उपलब्ध है।



# चैप्टर 7: ऑनलाइन आवाज़ उठाओ, बदलाव लाओ!

नूर हमेशा इंटरनेट को सिर्फ सीखने और मनोरंजन की जगह मानती थी, लेकिन अब उसकी सोच बदल रही थी। अब, जब वह अपनी नागरिक शास्त्र के प्रोजेक्ट पर काम कर रही थी, तो वह बार-बार यह सोच रही थी कि युवा लोग ऑनलाइन क्या भूमिका निभाते हैं—और वह जो कुछ भी सीख चुकी है, उसका बेहतर इस्तेमाल कैसे कर सकती है।

अमित भैया, मैं पिछले कुछ समय से सोच रही हूँ कि हम इंटरनेट का इस्तेमाल कैसे करते हैं। यह बहुत ज़बरदस्त है कि कैसे लोग ऑनलाइन जुड़कर बड़ा बदलाव ला सकते हैं, और सबसे अच्छी बात यह है कि उन आवाज़ों को भी जगह मिलती है जो आमतौर पर नहीं सुनी जातीं।



बिल्कुल! इंटरनेट एक ऐसी जगह है जहाँ हम सब मिलकर इसे बेहतर बना सकते हैं। अगर हम मेहनत करें, तो यह मज़ेदार और फायदेमंद दोनों हो सकता है!



मुझे भी इंटरनेट को एक सामुदायिक जगह मानना अच्छा लगता है! सच में, जैसे हम भारत के नागरिक हैं, वैसे ही क्या हम डिजिटल दुनिया के नागरिक नहीं हैं?



हाँ! समान अधिकारों और जिम्मेदारियों के साथ!



सही कहा! सोच रही हूँ, अगर डिजिटल नागरिकों के लिए एक प्रस्तावना बनाई जाए, तो वह कैसी होगी?



## एक डिजिटल नागरिक के रूप में जिम्मेदारियाँ

नूर ने एक प्रस्तावना तैयार की जिसमें कुछ ऐसे बिंदु शामिल थे जिन पर कोई समझौता नहीं किया जा सकता और उसके मुताबिक सभी डिजिटल नागरिकों को उनका पालन करना चाहिए। अपने दोस्तों के साथ चर्चा करें और दो जिम्मेदारियाँ जोड़ें जो आपको लगता है कि यहाँ शामिल की जानी चाहिए!

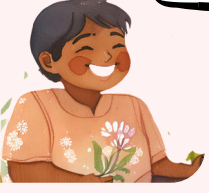
हम, डिजिटल दुनिया के नागरिक, यह संकल्प लेते हैं कि हम अपने ऑनलाइन व्यवहार में न्याय, स्वतंत्रता और समानता को बनाए रखेंगे, और इसके लिए अपनी प्रतिबद्धता घोषित करते हैं।

- सभी की राय और अधिकारों का सम्मान करेंगे, ताकि हर आवाज़ गरिमा और निष्पक्षता के साथ सुनी जाए।
- सभी की गोपनीयता का सम्मान करेंगे और उनके व्यक्तिगत स्पेस को दखल या गलत इस्तेमाल से बचाएंगे।
- जो भी जानकारी साझा करेंगे, पहले उसकी सच्चाई परखेंगे, ताकि सत्य और ईमानदारी बनी रहे।
- डिजिटल दुनिया में अपनी जिम्मेदारी समझेंगे और भरोसे और जवाबदेही का माहौल बनाएंगे।
- हमेशा अच्छे व्यवहार और शिष्टाचार का पालन करेंगे, विनम्रता, सहानुभूति और परस्पर सम्मान के साथ जुड़ेंगे।

अपने अधिकारों और जिम्मेदारियों को एक साथ निभाते हुए, हम एक समावेशी, सुरक्षित और सार्थक डिजिटल दुनिया बनाने का प्रयास करेंगे, जहाँ हर कोई स्वतंत्रता, जिम्मेदारी और उद्देश्य के साथ जुड़ सके।

## परिवर्तनकर्ता

नूर! तुमने जो डिजिटल नागरिकों के लिए प्रस्तावना बनाई है, वह वायरल हो गई है! स्कूल में हर कोई इसके बारे में बात कर रहा है!



हमारी नागरिक शास्त्र की क्लास में अधिकारों और जिम्मेदारियों के बारे में चर्चा हुई, और बहुत से लोगों ने डिजिटल नागरिकता का मुद्दा भी उठाया!



धन्यवाद दोस्तों!



यह तो कमाल है! तुम लोगों को अपने ग्रुप से बाहर भी इस बातचीत को बढ़ावा देते देख तो मुझे मज़ा आ गया !



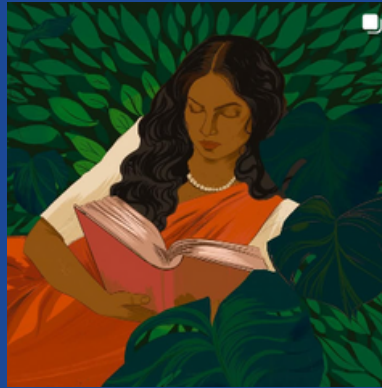
मलीहा अबीदी जैसी? उन्होंने जो किया वह बहुत प्रेरणादायक है! मैं भी सोच रही थी कि मैं ऐसा क्या कर सकती हूँ जिससे कोई ज़रूरी बदलाव आ सके!



मुझे यकीन है कि तुम यह ज़रूर कर सकती हो! लेकिन ये मलीहा आबिदी है कौन और क्या करती हैं?



मलीहा आबिदी 23 वर्षीय कलाकार और लेखिका हैं। वह कराची से हैं, और फ़िलहाल में ससेक्स विश्वविद्यालय में न्यूरोसाइंस की पढ़ाई कर रही हैं, साथ ही अपने अलग अलग प्रोजेक्ट्स के ज़रिये कला और महिला सशक्तिकरण के लिए अपने जुनून को जारी रखती हैं, उनमें से एक उनकी नयी किताब "पाकिस्तान फॉर वीमेन" है।





क्या बात है! लोग इंटरनेट का उपयोग कितने कमाल के कामों के लिए कर रहे हैं!

हाँ बिल्कुल! और ऑनलाइन संसाधन उन मुद्दों को बेहतर समझने में बहुत मदद करते हैं, जिनकी मुझे परवाह है!



- बहुत सारे ऑनलाइन प्लेटफॉर्म विद्यार्थियों की पढ़ाई में मदद करते हैं। ये स्कूल के सब्जेक्ट्स का स्टडी मटेरियल, बोर्ड और एंट्रेस एजाम की तैयारी, ट्यूशन और होमवर्क में मदद जैसी सुविधाएँ देते हैं।
- हम ऑनलाइन रिसोर्सेज का इस्तेमाल करके उन विषयों और मुद्दों के बारे में भी सीख सकते हैं, जिनमें हमारी दिलचस्पी है। रिसर्च पढ़कर और उस क्षेत्र के लोगों की बातें सुनकर हम उन्हें बेहतर समझ सकते हैं।

## सीखना और बढ़ना



पिछले हफ्ते ही सिद्धार्थ ने क्राउडफंडिंग का इस्तेमाल करके अपने एक दोस्त के मेडिकल खर्च के लिए पैसे जुटाए थे। हम एक-दूसरे के लिए आगे आ सकते हैं और मदद कर सकते हैं!



## साथियों और समुदाय के लिए जागरूकता और समर्थन

- सोशल मीडिया मोबिलाइज़ेशन – एक्टिविस्ट्स मशहूर सोशल मीडिया और मैसेजिंग प्लेटफॉर्म का इस्तेमाल तेजी से मैसेज फैलाने, वायरल कैंपेन शुरू करने और बड़े पैमाने पर लोगों को जोड़ने के लिए करते हैं। हैशटैग, लाइव वीडियो और डिजिटल पेटिशन किसी भी मुद्दे को आगे बढ़ाने में मदद करते हैं, जिससे लोगों को जोड़ना और जनता के बीच बातचीत शुरू करना आसान हो जाता है।
- समुदायिक समन्वय और सीधी कार्रवाई – ऑर्गेनाइज़र ऑनलाइन फोरम, मेलिंग लिस्ट और मैसेजिंग ऐप्स का उपयोग प्लानिंग, संसाधनों को शेयर करने और लोगों को जोड़े रखने के लिए करते हैं। क्राउडसोर्सिंग प्लेटफॉर्म और डिजिटल साइन-अप, सामूहिक एक्शन को आसान बनाते हैं, जिससे लोग किसी मुद्दे के प्रति अपना साथ और विश्वास जता सकते हैं और पैसे का योगदान दे सकते हैं!



## परिवर्तनकर्ता

यह वाकई अद्भुत है कि हम ऑनलाइन कितनी चीजें सीख सकते हैं और कर सकते हैं, लेकिन इसका मतलब यह भी है कि इसे एक बेहतर जगह बनाने की जिम्मेदारी हमारी है, है ना?



हाँ, बिल्कुल! यह सिर्फ इंटरनेट के इस्तेमाल के बारे में नहीं है, बल्कि यह भी है कि हम दूसरों के साथ कैसे बात करते हैं और यह सुनिश्चित करते हैं कि यह एक अच्छी जगह बनी रहे।



क्या हम किसी को पोस्ट करने या जवाब देने से पहले सोचने के लिए कुछ बातें लिख सकते हैं?



बढ़िया आईडिया है! मुझे लगता है इंटरनेट की सबसे अच्छी बातों में से एक ये है कि हम उन लोगों की बातें सुन सकते हैं जिन्हें हम आमतौर पर समाचारों या टीवी पर नहीं देखते।



हाँ, लेकिन मैंने यह भी देखना शुरू कर दिया है कि कुछ लोगों को ऑनलाइन बहुत ज़्यादा नफ़रत मिलती है। मुझे लगता है कि हमें कुछ करना चाहिए - चाहे वो रिपोर्ट करना हो, बोलना हो या बस समर्थन दिखाना हो।



### सहज और संवेदनशील बातचीत

- क्या यह अच्छा है? (क्या इससे किसी को अच्छा महसूस होगा या बुरा?)
- क्या यह ज़रूरी है? (क्या मुझे सच में यह कहना चाहिए?)
- क्या यह सम्मानजनक है? (अगर कोई मुझसे यह कहे, तो क्या मुझे ठीक लगेगा?)
- क्या यह सही है? (क्या मैंने इसकी सटीक जानकारी जांची है?)
- क्या यह गोपनीयता का सम्मान करता है? (क्या मैं बिना अनुमति के किसी की निजी जानकारी शेयर कर रहा/रही हूँ?)

### समर्थन व्यक्त करना

- सामना करें - अगर सुरक्षित लगे, तो सही जानकारी या शांत प्रतिक्रिया देकर गलत और हानिकारक कमेंट को चुनौती दें।
- रिपोर्ट करें और ब्लॉक करें - प्लेटफॉर्म के टूल्स का इस्तेमाल करके हेट स्पीच की रिपोर्ट करें और आगे होने वाले नुकसान को रोकें।
- दयालुता को बढ़ावा दें - बातचीत का रुख बदलें और सम्मानजनक व समावेशी चर्चा को प्रोत्साहित करें।



## बातचीत और बदलाव की ओर कदम

सही बात है!! हम ऑनलाइन भी वैसे ही हो सकते हैं जैसे हम असल जिंदगी में होते हैं। लेकिन सिर्फ अपनी गतिविधियों में सावधानी बरतने के अलावा, क्या हम इंटरनेट को एक बेहतर जगह बनाने के लिए और कुछ कर सकते हैं?

हाँ! हम सभी अलग-अलग ग्रुप्स का हिस्सा हैं- हमारे परिवार, स्कूल, यहाँ तक कि ऑनलाइन समुदाय भी। हमने जो सीखा है उसे उन जगहों पर भी लाने के तरीके होने चाहिए, है न?

बिल्कुल! ऐसी कई चीजें हैं जो हम अलग-अलग स्तरों पर कर सकते हैं - घर पर, अपने स्कूलों में, अपने दोस्तों के बीच और यहाँ तक कि बड़े ऑनलाइन स्पेस में भी। यह सब मिलकर काम करता है!

**बदलाव घर से शुरू होता है!**

- छोटे भाई-बहनों या परिवार के सदस्यों को गोपनीयता सेटिंग्स और डिजिटल देखभाल के बारे में सिखाएं।
- माता-पिता को फर्जी खबरों या ऑनलाइन धोखाधड़ी की पहचान करने में सहायता करें।
- स्क्रीन पर समय बिताने की स्वस्थ आदतों के बारे में बातचीत शुरू करें।

**एक सच्चा मित्र**

- हानिकारक जोक्स, साइबरबुलिंग या अनुचित कंटेंट पर आवाज उठाएँ।
- अगर कोई दोस्त ऑनलाइन असुरक्षित या परेशान महसूस कर रहा है, तो उसका समर्थन करें।
- दूसरों को याद दिलाएँ कि किसी भी जानकारी को शेयर करने से पहले उसकी सच्चाई जांच लें।

## स्कूल में एंबेसडर बनें



- डिजिटल दयालुता अभियान शुरू करें – जहाँ स्टूडेंट्स एक-दूसरे के लिए पॉजिटिव मैसेज पोस्ट करें।
- जागरूकता क्लब बनाएं – ऑनलाइन सेफ्टी और डिजिटल अधिकारों पर चर्चा करने के लिए एक ग्रुप शुरू करें।
- शिक्षकों के साथ मिलकर काम करें – जिम्मेदार इंटरनेट इस्तेमाल पर वर्कशॉप आयोजित करें और स्टूडेंट एंबेसडर्स की पहचान करें।

## समुदाय के साथ बातचीत

- स्थानीय ग्रुप्स में ऑनलाइन धोखाधड़ी और गलत जानकारी पर जागरूकता फैलाएं।
- स्कूलों और युवाओं के लिए सुरक्षित ऑनलाइन नीतियों को मजबूत करने के लिए आवाज उठाएं।
- मानसिक स्वास्थ्य, ऑनलाइन उत्पीड़न और सहायता नेटवर्क से जुड़ी प्रमाणित जानकारियाँ दूसरों तक पहुँचाएँ।



ये तो बहुत बढ़िया आइडियाज़ हैं, शुभम! हमारा ऑनलाइन भविष्य उतना ही हमारे फैसलों पर निर्भर करता है, जितना कि इंटरनेट हमारे ऑनलाइन अनुभवों को बदलता है।



ठीक है! मैं सबको बता दूँगी कि हम कल दोपहर को मिल रहे हैं!

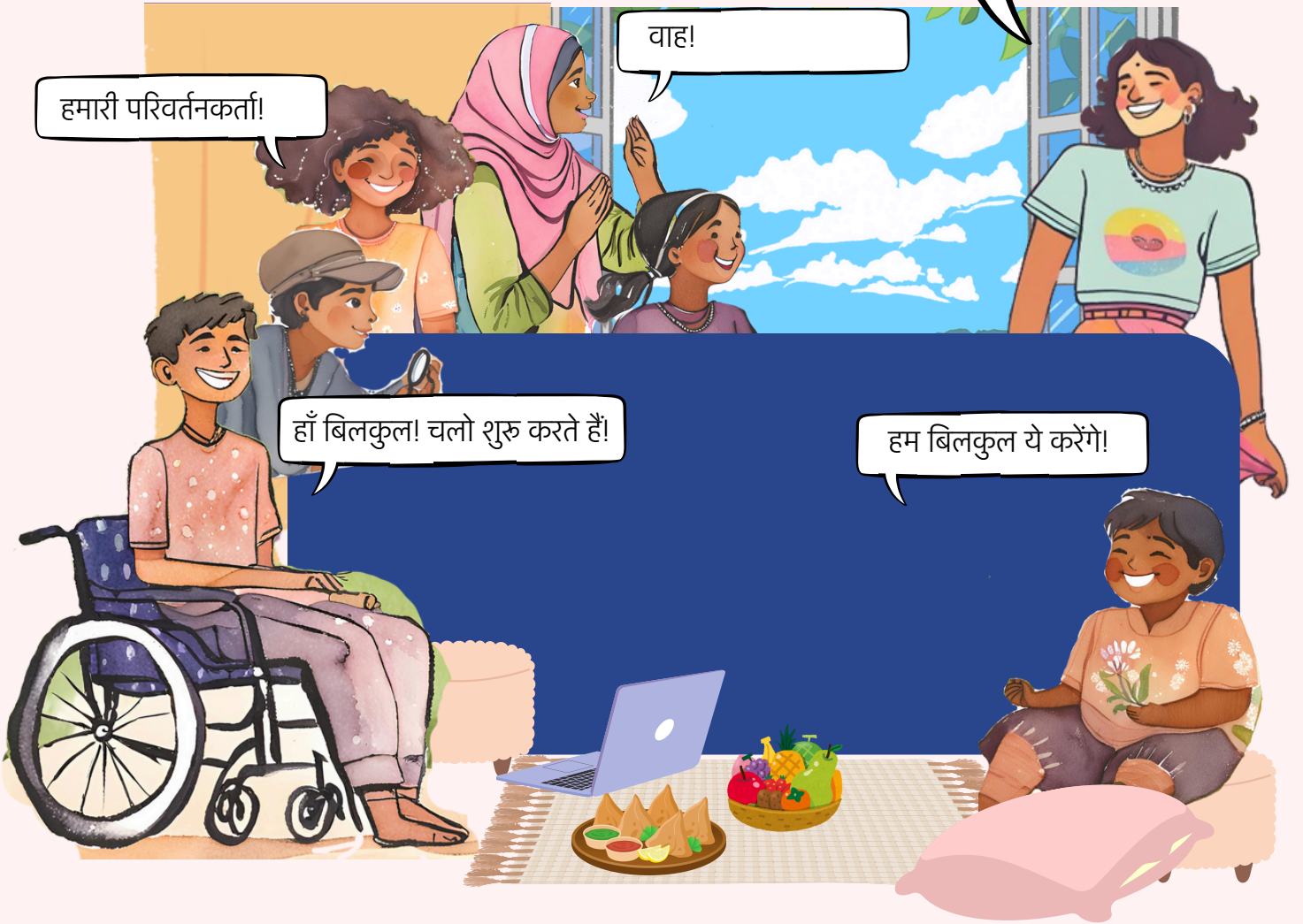


बिल्कुल सही! अब मेरे दिमाग में एक नया आइडिया आया है, जिसे मैं आजमाना चाहती हूँ – नूर, मुझे तुम्हारी मदद चाहिए!!



एक बार फिर, सभी दोस्त साथ आ गए थे। लेकिन इस बार, यह सिर्फ़ मस्ती भरी दोपहर नहीं थी। शुभम के पास टीम के लिए एक खास मिशन था, और सब बेसब्री से सुनने के लिए तैयार थे।

हर क्लिक, कमेंट और शेयर उस इंटरनेट को बनाता है जिसे हम सभी इस्तेमाल करते हैं। तो क्या तुम अपनी आवाज़ उठाकर बदलाव लाना और अपने समुदाय में एक नई पहल शुरू करना चाहते हो?



शुभम ने सभी को वर्कशीट और पेन दिए, साथ ही उनकी सोच को दिशा देने के लिए एक मिशन स्टेटमेंट भी दिया। मिशन स्टेटमेंट देखने के लिए नीचे स्क्रोल करें और देखें कि 30 मिनट में उन्होंने क्या किया! उनकी अंतिम कार्य योजना देखने के लिए स्क्रोल करते रहें।



सुरक्षा नगर के रक्षकों,

आपका समुदाय आपको बुला रहा है। कचरे और प्रदूषण का बढ़ता खतरा हमारी सड़कों, हमारी हवा और हमारे भविष्य को नुकसान पहुँचा रहा है। यह समय है कुछ कर दिखने का—अपने साथियों को इकट्ठा करें, जागरूकता फैलाएँ और इस समस्या का हल बनें। जागरूकता अभियानों से लेकर सफाई अभियान तक, हर कदम मायने रखता है।

मिशन साफ़ है: सुरक्षा नगर को फिर एक बार सुरक्षित और साफ़ बनाना।

क्या आप इस चुनौती को स्वीकार करेंगे? अगर आप बदलाव लाने के लिए तैयार हैं, तो अभी अपनी कार्ययोजना बनाइए!



 **TAKE  
ACTION**

 **WORK  
TOGETHER!**

 **USE YOUR  
voice  
FOR CHANGE**



लक्ष्य: सामुदायिक प्रयास और डिजिटल जागरूकता के ज़रिए सुरक्षा नगर को साफ़ और सुरक्षित बनाना।

1 महीना – जागरूकता अभियान + 2 साप्ताहिक सफाई अभियान + लगातार सोशल मीडिया पर अभियान के अपडेट शेयर करना

### शुभम – क्रिएटिव डिज़ाइनर

- Canva का इस्तेमाल करके पोस्टर बनाना सीखें।
- कैंपेन के हैशटैग के साथ आकर्षक विजुअल्स तैयार करें और इसे ऑनलाइन व समुदाय में शेयर करें।

### रहीम – Reel मेकर

- प्रदूषण की समस्या और समुदाय के प्रयासों को दिखाने वाले छोटे-छोटे रीलस शूट और एडिट करें।
- सोशल मीडिया पर वीडियो पोस्ट करके जागरूकता फैलाएँ।

### सुजैन – कम्युनिटी कनेक्टर

सुरक्षा नगर के मैसेजिंग ग्रुप को मैनेज करें। पड़ोसियों को जोड़ें, अपडेट्स शेयर करें और सभी को सफाई अभियानों की याद दिलाएँ।

### जसप्रीत – हैशटैग हीरो

- #CleanSuraksha हैशटैग को मॉनिटर करें।
- लोगों को प्रोत्साहित करें कि वे अपने सफाई अभियानों को इस हैशटैग के साथ शेयर करें, ताकि सामूहिक प्रयास की भावना मजबूत हो सके।

### मीरा – सोशल मीडिया कैप्टन

- @CleanSuraksha जैसी एक कैंपेन पेज बनाएँ और चलाएँ।
- नियमित रूप से अपडेट पोस्ट करें, सफलता की कहानियाँ शेयर करें, और लोगों को योगदान देने के तरीके बताएँ।

### सिद्धार्थ – रिसर्चर & इनफॉर्मर

- प्रदूषण, कचरा प्रबंधन और पर्यावरण के अनुकूल आदतों पर रिसर्च करें।
- जानकारीपूर्ण पोस्ट लिखें और रोज़मर्रा की ज़िंदगी में कचरा कम करने के टिप्स शेयर करें।

### नूर – इवेंट ऑर्गनाइज़र

- सफाई अभियान और जागरूकता इवेंट्स की प्लानिंग और कोऑर्डिनेशन करें।
- वॉलंटियर्स के लिए डिजिटल साइन-अप फॉर्म और शेड्यूल तैयार करें।

अपना खुद का मिशन तय करें और जिस मुद्दे की आपको परवाह है, उसे हल करने के लिए एक योजना बनाएं!

उद्देश्य:






लक्ष्य:

समयरेखा:

गतिविधियाँ:

नियम और जिम्मेदारियाँ:

## चैप्टर रिकैप

-  डिजिटल दुनिया में हमारे पास अधिकार भी हैं और ज़िम्मेदारियाँ भी - जैसे दूसरों की राय, अधिकार और प्राइवैसी का सम्मान करना।
-  इंटरनेट एक शक्तिशाली माध्यम बन सकता है! इसका इस्तेमाल दुनिया में बदलाव लाने के लिए अपनी आवाज़ उठाने में करें।
-  इंटरनेट से आप सीख सकते हैं, नए दोस्त बना सकते हैं, और दूसरों की मदद कर सकते हैं।
-  हमेशा खुद से पूछें, क्या मेरे शब्द और काम सौम्य हैं? क्या वे सम्मानजनक हैं?
-  बदलाव घर से शुरू होता है! अपने परिवार और दोस्तों से बात करें, स्कूल में एंबेसडर बनें, और गलत व्यवहार का विरोध करें।

# BIBLIOGRAPHY

## Chapter 1

- 88% of kids watch online videos- Global kids online report MICA
- World's First Website.
- How many websites are there?
- The weight of the internet.
- Number of People using Google.
- The first emoji ever created.

## Chapter 2

- Cyber Security - Awareness for Citizens. Cyber Crime Portal.
- Don't fall prey to these scams! 10 common ways in which scamsters can fraud you.
- 3. Minding the data: Protecting learners' privacy and security.

## Chapter 3

2

- Different types of Bullying
- What are cyber crimes?
- Respecting Privacy
- Cache and cookies:

## Chapter 4

- Rest assured, salt is not poisoning you.
- Evaluating Resources and Misinformation.
- How do algorithms work?
- How does AI work? Basics to know.

## Chapter 5

- National Cyber Crime Reporting Portal
- Online Hate and free speech
- IT Laws India

# BIBLIOGRAPHY

## Chapter 6

- Mental health resources
- A commitment planner to balance your time use.
- How to identify and help a friend struggling with mental health issues

## Chapter 7

- Safetinterview with Maliha Abidi
- Using internet based tools to promote community health and development
- Digital Safety and Citizenship Curriculum

