शिक्षक व अभिभावक जागरूकता सत्र

संज्ञानात्मक सुरक्षा और मानव मनोविज्ञान

बच्चों को मानसिक हेरफेर, गलत सूचना और ऑनलाइन जोखिमों से बचाना सीखें

परिचय

संज्ञानात्मक सुरक्षा क्या है?

दिमाग को उन कोशिशों से बचाना जो हमारी सोच, राय और फैसलों को गलत तरीके से प्रभावित करने के लिए की जाती हैं।

जिस तरह हम बच्चों को सड़क पार करना सिखाते हैं, उसी तरह आज उन्हें यह भी सिखाना ज़रूरी है कि ऑनलाइन दुनिया में कौन सच में मदद कर रहा है और कौन उनकी सोच से खेल रहा है।

शिक्षक और अभिभावक — बच्चे की पहली सुरक्षा परत

बच्चे ज़्यादा संवेदनशील क्यों?

- सबसे ज़्यादा समय ऑनलाइन बिताने वाली पीढ़ी
- दिमाग अभी विकसित हो रहा होता है
- भावनात्मक दबाव और बहकावे के प्रति ज़्यादा संवेदनशील
- असली और नकली में फर्क करने का अनुभव कम

सत्र की रूपरेखा

आज हम क्या-क्या सीखेंगे

01 संज्ञानात्मक सुरक्षा क्या है — बच्चों के लिए क्यों ज़रूरी

02 संज्ञानात्मक पूर्वाग्रह और निर्णय लेना

03 प्रभाव अभियान और मनोवैज्ञानिक हेरफेर

04 ध्यान, धारणा और सूचना का अत्यधिक बोझ

05 शिक्षकों व अभिभावकों के लिए व्यावहारिक कदम

06 रिपोर्टिंग संसाधन और हेल्पलाइन

मुख्य आंकड़े

89.1%

14-16 वर्ष के किशोरों के घर में स्मार्टफोन (ASER 2024)

900%

भारत में डीपफेक मामलों में वार्षिक वृद्धि

6x

गलत सूचना सही खबर से जितनी तेज़ फैलती है

स्रोत: ASER 2024 / UNICEF India (2026); Kaval Misinformation Report (2026); MIT अध्ययन

भारतीय मस्तिष्क की सुरक्षा:

संज्ञानात्मक रक्षा की ओर बदलाव

प्रतिमान में बदलाव (Paradigm Shift)

भारत की हमला-सतह अब केवल सर्वर और नेटवर्क तक सीमित नहीं है। यह एक अरब जुड़े हुए नागरिकों का मस्तिष्क है।

खतरा (Threat)

गलत सूचना केवल एक कंटेंट-मॉडरेशन समस्या नहीं है। यह मानव अर्थ-निर्माण को हाईजैक करने, राजनीतिक ध्रुवीकरण बढ़ाने और समाज को अस्थिर करने के लिए इंजीनियर किया गया एक न्यूरोबायोलॉजिकल खतरा है।

समाधान (The Solution)

भारतीय दर्शन और इंजीनियर्ड 'फ्रिक्शन' में निहित एक 'संपूर्ण-राष्ट्र' संज्ञानात्मक रक्षा रणनीति। (Whole-of-nation defence strategy)

सुरक्षा प्रतिमान में बदलाव

दशकों से, सर्वर को सुरक्षित करने में अरबों खर्च हुए जबकि मानव अनुभूति (कॉग्निशन) पूरी तरह असुरक्षित रही। आधुनिक संज्ञानात्मक युद्ध कंप्यूटर को हैक नहीं करता — यह वास्तविकता को अनिश्चित महसूस कराने के लिए मानव के 'सत्य-डिफ़ॉल्ट' आधार का शोषण करता है।

निदान मैट्रिक्स (Diagnostic matrix)	पारंपरिक साइबर सुरक्षा	संज्ञानात्मक सुरक्षा
मुख्य सुरक्षित संपत्ति (Core Asset Protected)	मशीनें और नेटवर्क	**अनुभूति और अर्थ-निर्माण (perception & Sense-making)**
प्राथमिक खतरा (Primary)	मालवेयर और घुसपैठ (Malware & Intrusions)	**मनोवैज्ञानिक हेरफेर और ध्रुवीकरण (Psychological Manipulation & Polarization)**
मानव आधार रेखा (Human Baseline)	ज़ीरो-ट्रस्ट आर्किटेक्चर	**सत्य-डिफ़ॉल्ट -ईमानदारी की विकासवादी धारणा (Evolutionary Assumption of Honesty)**
रक्षा रणनीत (Defence Stragetegy) ि	फायरवॉल और कंटेंट फ़िल्टरिंग	**इंजीनियर्ड फ्रिक्शन और प्री-बंकिंग**

भारत की अरब-नोड हमला सतह

भारत एक अभूतपूर्व लक्ष्य प्रस्तुत करता है: पहली बार इंटरनेट उपयोग करने वाली एक विशाल जनसंख्या, जो बंद, एन्क्रिप्टेड एल्गोरिद्म और स्थानीय-भाषा (वर्नाक्युलर) की खामियों के माध्यम से दुनिया का अनुभव कर रही है।

1. स्तर और इको चैंबर

करोड़ों बंद-नेटवर्क उपयोगकर्ता जहाँ एल्गोरिदमिक माइक्रो-टार्गेटिंग फलती-फूलती है।

2. पहली बार की भेद्यता (Vulnerable First-timers)

विस्फोटक, देर से हुए डिजिटलीकरण का मतलब है कि लाखों लोगों के पास डिजिटल हेरफेर के खिलाफ अनुभव-आधारित संज्ञानात्मक 'एंटीबॉडी' नहीं हैं।

2010: 4 करोड़ उपयोगकर्ता
2020: 20 करोड़ उपयोगकर्ता
वर्तमान: 130 करोड़+ उपयोगकर्ता

3. भाषाई विखंडन (Linguistic Fragmentation)

स्थानीय भाषा (वर्नाक्युलर) में गलत सूचना अंग्रेज़ी या हिंदी सामग्री की तुलना में तेज़ी से फैलती है और धीमी गति से जाँची जाती है (हिंदी, मराठी, तेलुगु, बंगाली, तमिल आदि)।

बच्चों और किशोरों में आम पूर्वाग्रह

दिमाग के वे 'शॉर्टकट' जो फैसले जल्दी लेने में मदद करते हैं — और जिनका फायदा ऐप और ठग दोनों उठाते हैं

1

सामाजिक प्रमाण

'सबके पास है, सब खेल रहे हैं' — यही सोच किसी ट्रेंड में शामिल होने पर मजबूर करती है।

2

FOMO (छूट जाने का डर)

'आज ही खरीदें' जैसे संदेश जल्दबाज़ी में फैसला करवाते हैं।

3

वेरिएबल रिवॉर्ड

गेम में कभी इनाम मिलना, कभी नहीं — जुए जैसी अनिश्चितता बार-बार खेलने पर उकसाती है।

4

अथॉरिटी बायस

पसंदीदा इन्फ्लुएंसर या 'बड़े भाई/दीदी' जैसे अजनबी पर आंख मूंदकर भरोसा।

केस स्टडी

बेंगलुरु — गेमिंग ऐप में ₹1.87 लाख खर्च

कहां और कब	बेंगलुरु, फरवरी 2025
क्या हुआ	14 साल के बच्चे ने पिता के UPI से जुड़े फोन का इस्तेमाल कर सिर्फ 3 हफ्तों में गेमिंग करेंसी पर ₹1.87 लाख खर्च कर दिए।
मनोवैज्ञानिक हथकंडे	सीमित समय का ऑफर, 'मौका चला जाएगा' का डर, और बार-बार मिलने वाला अनिश्चित इनाम (variable reward)।
सबक	बच्चे को 'लालची' कहने की बजाय समझें कि गेम को ही ऐसे मनोविज्ञान पर डिज़ाइन किया गया है जो हर उम्र के लोगों को फंसा सकता है।

₹1.87

लाख रुपये — सिर्फ 3 हफ्तों में

स्रोत: RightToInformation.wiki
Child Online Safety Guide (2026)

मनोवैज्ञानिक हेरफेर के सामान्य पैटर्न

1	**धीरे-धीरे भरोसा बनाना**	तारीफ या छोटे तोहफों से भरोसा जीतकर फिर निजी जानकारी मांगना।
2	**गोपनीयता और अलगाव**	'यह बात किसी को मत बताओ' — परिवार-दोस्तों से दूर करने की कोशिश। यही सबसे बड़ा चेतावनी संकेत है।
3	**भावनात्मक ट्रिगर**	डर, शर्म, जिज्ञासा या अकेलापन जगाकर जल्दी प्रतिक्रिया करवाना।
4	**गलत सूचना व फॉरवर्ड**	WhatsApp और सोशल मीडिया पर बिना जांचे फैले संदेश।
5	**AI-जनित फर्जी सामग्री**	असली दिखने वाली नकली तस्वीरें या वीडियो (डीपफेक) बनाकर शर्मिंदा करना।

भारत में गलत सूचना और ऑनलाइन जोखिम

53.5 करोड़+

भारत में WhatsApp उपयोगकर्ता — हर 3 में 1 भारतीय; एन्क्रिप्शन से गलत सूचना पर नियंत्रण मुश्किल

~66%

अमेरिकी शिक्षकों ने कहा — उनके छात्र डीपफेक सामग्री से गुमराह हो चुके हैं

40–50%

छात्र स्कूल में डीपफेक सामग्री के प्रसार के बारे में जानते हैं

स्रोत: Kaval Misinformation Report (2026); NEA/NEARI (2025); The Conversation (2023)

अजनबियों से जुड़ा पैटर्न — पहचानें और रिपोर्ट करें

ऑनलाइन दोस्ती बनाने वाले अजनबियों का एक जाना-पहचाना पैटर्न होता है — **तारीफ या छोटे तोहफों से भरोसा बनाना, धीरे-धीरे निजी बातचीत बढ़ाना, और फिर बच्चे को चुप कराने की कोशिश करना।** परिवार से गोपनीयता रखने की मांग हमेशा सबसे बड़ा चेतावनी संकेत है।

केस: पुणे (जनवरी 2025)

एक सतर्क मां ने समय रहते संदेह होने पर डिजिटल सबूत जुटाए और POCSO अधिनियम के तहत FIR दर्ज करवाई, जिससे 48 घंटे के भीतर गिरफ्तारी हुई। पैटर्न को जल्दी पहचानना और तुरंत रिपोर्ट करना कितना असरदार हो सकता है — यही इस मामले का सबक है।

बच्चे को बिना डर के अजीब या असहज अनुभव साझा करने दें — पहली प्रतिक्रिया हमेशा साथ और समाधान होनी चाहिए, डांट नहीं।

स्रोत: RightToInformation.wiki, Child Online Safety Guide (2026)

ध्यान, धारणा और सूचना का अत्यधिक बोझ

1

ध्यान (Attention)

ऐप्स और गेम जानबूझकर ध्यान बंटाने के लिए डिज़ाइन होते हैं — नोटिफिकेशन, ऑटो-प्ले, लगातार स्क्रॉल।

2

धारणा (Perception)

असली-नकली, विज्ञापन-सच्ची जानकारी और दोस्त-अजनबी में फर्क समझने की क्षमता अभी विकसित हो रही होती है।

3

सूचना का बोझ

स्कूल, पारिवारिक और सोशल मीडिया संदेशों की बाढ़ में जांचने का समय नहीं मिलता — गलत सूचना पर भरोसा बढ़ता है।

ठग अक्सर परीक्षा के समय, छुट्टियों या त्योहारों के आसपास सक्रिय होते हैं — जब सावधानी से सोचने का समय सबसे कम होता है।

आंकड़े: ध्यान और सूचना का बोझ

47 सेकंड

स्क्रीन पर औसत ध्यान अवधि — 2004 में 2.5 मिनट थी

76%

किशोर स्मार्टफोन मुख्यतः सोशल मीडिया के लिए इस्तेमाल करते हैं, सिर्फ 57% पढ़ाई के लिए

90%

लोग हफ्ते में कम-से-कम एक बार 'सूचना बोझ' का अनुभव करते हैं

स्रोत: ASER 2024 / UNICEF India (2026); Kaval Misinformation Report (2026); WifiTalents (2026)

एक संपूर्ण-राष्ट्र आर्किटेक्चर

मस्तिष्कों की रक्षा किसी एक मंत्रालय या तकनीकी प्लेटफ़ॉर्म को नहीं सौंपी जा सकती। इसके लिए एक एकीकृत आर्किटेक्चर चाहिए जहाँ स्वास्थ्य संचार, तकनीकी फ्रिक्शन और राष्ट्रीय सुरक्षा योजना एक साथ, तालमेल में काम करें।

सरकार व संस्थान
राष्ट्रीय संज्ञानात्मक सुरक्षा केंद्र, एकीकृत सिद्धांत

टेक प्लेटफ़ॉर्म
इंजीनियर्ड फ्रिक्शन, एल्गोरिदमिक जवाबदेही

स्कूल और शिक्षक
NCERT/CIET संज्ञानात्मक लचीलापन पहल

नागरिक समाज व मीडिया
स्थानीय-भाषा सामुदायिक प्री-बंकिंग

व्यक्तिगत नागरिक
सजगता, भावनात्मक ट्रिगर के प्रति जागरूकता

शिक्षकों के लिए — कक्षा में क्या करें

1 **मीडिया साक्षरता पढ़ाएं**

शेयर करने से पहले स्रोत जांचने की आदत सिखाएं।

2 **खुली चर्चा को बढ़ावा दें**

बच्चे बिना डर के असहज बात साझा कर सकें, ऐसा माहौल बनाएं।

3 **असली केस स्टडी पर चर्चा करें**

उदाहरणों से बच्चे पैटर्न पहचानना सीखते हैं।

4 **रिपोर्टिंग प्रक्रिया सिखाएं**

बच्चों को पता हो कि स्कूल में किससे शिकायत करनी है।

अभिभावकों के लिए — घर पर क्या करें

1 रुकें, सोचें, जांचें

डराने वाला संदेश मिलने पर परिवार में मिलकर सच्चाई जांचें।

2 भावनात्मक ट्रिगर पहचानना सिखाएं

डर, लालच, गोपनीयता का दबाव — ये सभी चेतावनी संकेत हैं।

3 'बिना डांट के बातचीत' का माहौल

गलती होने पर पहली प्रतिक्रिया सज़ा नहीं, साथ मिलकर समाधान हो।

4 स्क्रीन-टाइम समझौता मिलकर बनाएं

कब, कितनी देर, किन ऐप्स का इस्तेमाल होगा — यह साथ तय करें।

रिपोर्टिंग संसाधन और हेल्पलाइन

1930

नेशनल साइबर क्राइम हेल्पलाइन — किसी भी संदिग्ध घटना की तुरंत रिपोर्ट करें

cybercrime.gov.in

ऑनलाइन शिकायत दर्ज करने का सरकारी पोर्टल

POCSO ई-बॉक्स

बच्चों से जुड़े यौन अपराध मामलों की गोपनीय रिपोर्टिंग

NCPCR

नेशनल कमीशन फॉर प्रोटेक्शन ऑफ चाइल्ड राइट्स से सहायता

मुख्य सीख

1. संज्ञानात्मक पूर्वाग्रह बच्चों की 'गलती' नहीं, दिमाग का स्वाभाविक हिस्सा हैं — इन्हें पहचानना ही सबसे पहला बचाव है।

2. ऐप, गेम और ठग तीनों एक ही मनोविज्ञान का इस्तेमाल करते हैं — तात्कालिकता, भरोसा और गोपनीयता का दबाव।

3. ध्यान और सूचना के बोझ को समझना उतना ही ज़रूरी है जितना पासवर्ड सुरक्षित रखना सिखाना।

4. मानसिक प्रतिरोध क्षमता एक कौशल है — डांट से नहीं, खुली बातचीत और नियमित अभ्यास से बनती है।

5. समय रहते पैटर्न पहचानना और तुरंत रिपोर्ट करना बड़े नुकसान को रोक सकता है।

धन्यवाद

“बच्चों को हर खतरे से बचाना संभव नहीं, लेकिन उन्हें पहचानना सिखाना हमेशा संभव है।”