

# साइबर सुरक्षा के दिशानिर्देश

अभिभावकों हेतु

संस्करण -1.1



# विकाश समिति

## अध्यक्ष

प्रोफ़ेसर अमरेन्द्र प्रसाद बेहेरा, संयुक्त निदेशक, केंद्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली।

## सदस्य समन्वयक

डॉ. एंजेल रत्नाबाई, सहायक प्रोफ़ेसर, केन्द्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली।

## सदस्य

डॉ. अंजुम सिबिया, प्रोफ़ेसर और हेड, डिवीज़न ऑफ़ एजुकेशनल रिसर्च (डीईआर), एनसीईआरटी, नई दिल्ली।

डॉ. इंदु कुमार, प्रोफ़ेसर और प्रमुख, डीआईसीटी और टीडी, केंद्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली।

सुश्री कुनिका, जूनियर प्रोजेक्ट फेलो, केंद्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली।

## डिज़ाइनर

संजय यादव, ग्राफ़िक अर्टिस्ट, मीडिया प्रोडक्शन डिपार्टमेंट, केंद्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली।



# बीज-शब्दावली

**साइबरबुलिंग** - आमतौर पर एक व्यक्ति को डराने या धमकी देने के लिए इलेक्ट्रॉनिक संचार का उपयोग कर मेसेज भेजना।

**ट्रोलिंग** - ट्रोलिंग को इंटरनेट पर भड़काऊ या ऑफ़-टॉपिक संदेशों को ऑनलाइन समुदाय में पोस्ट करके झगड़े शुरू करने या लोगों को परेशान करके कलह पैदा करने के रूप में परिभाषित किया गया है।

**फिशिंग** - इलेक्ट्रॉनिक संचार में अपनी पहचान छिपाकर एक भरोसेमंद इकाई के रूप में उपयोगकर्ता का नाम, पासवर्ड और क्रेडिट कार्ड विवरण जैसी संवेदनशील जानकारी प्राप्त करने के लिए धोखाधड़ी का प्रयास फिशिंग है।

**मैलवेयर** - मैलवेयर कोई भी सॉफ्टवेयर जिसको जानबूझकर कंप्यूटर, सर्वर, क्लाउंट या कंप्यूटर नेटवर्क को नुकसान पहुंचाने के लिए बनाया गया है।

**स्टाकिंग** - किसी व्यक्ति या समूह द्वारा दूसरे व्यक्ति की अवांछित या बार-बार निगरानी, स्टाकिंग है।

**रैनसमवेयर** - रैनसमवेयर एक प्रकार का नुकसानदायक सॉफ्टवेयर या मैलवेयर है, जिसे किसी कंप्यूटर सिस्टम या डाटा तक पहुंचने से रोकने के लिए डिजाइन किया गया है; जब तक कि फिरौती का भुगतान नहीं जाता हो। यह आमतौर पर फिशिंग ईमेल के माध्यम से या अनजाने में एक संक्रमित वेबसाइट पर जाकर फैलता है।

**वर्चुअल प्राइवेट नेटवर्क** - वर्चुअल प्राइवेट नेटवर्क एक सार्वजनिक इंटरनेट कनेक्शन के द्वारा एक निजी नेटवर्क बनाकर आपको ऑनलाइन गोपनीयता और गुमनामी प्रदान करता है। वीपीएन आपके इंटरनेट प्रोटोकॉल (आईपी) के पते को छिपाता है ताकि आपका ऑनलाइन कार्य ट्रैक न हो सके।

**अभिभावक के अंकुश** - अभिभावक के अंकुश में ऐसी विशेषताएं हैं, जिसमें माता-पिता को डिजिटल टेलीविजन सेवाओं, कंप्यूटर और वीडियो गेम, मोबाइल उपकरणों और सॉफ्टवेयर सामग्री को अपने बच्चों की पहुंच से प्रतिबंधित करने की अनुमति होती है।

# अंतर्वस्तु

- 1 परिचयात्मक विचार 01
- 2 बच्चों में देखी जाने वाली डिजिटल आदतें और उनके प्रभाव 02
- 3 डिजिटल युग में पालन-पोषण के लिए दिशानिर्देश 05
- 4 साइबर सुरक्षा पर अक्सर पूछे जाने वाले कुछ प्रश्न 13
- 5 भारतीय बच्चों की ऑनलाइन गतिविधि के बारे में आंकड़े 15
- 6 समापन के अवसर 23

वर्तमान में हम जिस 'साइबर युग' में जी रहे हैं, हम सभी अपने आप को डिजिटल दुनिया के नागरिक कह सकते हैं। प्रौद्योगिकी आज कुशल, व्यापक और सस्ती हो गई है। आज अधिकांश परिवारों और घरों में डिजिटल गैजेट्स का उपयोग एक नया प्रतिमान है। परिवार के सदस्य डिजिटल उपकरणों का उपयोग परिवार और दोस्तों से जुड़ने से लेकर ऑनलाइन लेन-देन करने तथा कर्गों का भुगतान करने में भी करते हैं। डिजिटल उपकरणों की सुविधा के माध्यम से प्रौद्योगिकी तक पहुँच बहुत दूर तक हो गई है और इसने हमारे दैनिक जीवन के हर पहलू को छू लिया है।

इस परिदृश्य में यह बहुत स्पष्ट है कि वर्तमान और भविष्य की पीढ़ी वही है जिस पर प्रौद्योगिकी का अमित प्रभाव होगा। आज बहुत कम उम्र के बच्चे डिजिटल गैजेट्स का उपयोग करते हैं। वे हर गतिविधि के क्षेत्र में उनका व्यावहारिक रूप से उपयोग करते हैं। आज बच्चे उपकरणों पर बहुत निर्भर हैं, जल्दी से डिजिटल उपकरणों के विभिन्न माध्यमों के अनुकूल हो जाते हैं और स्वाभाविक रूप से स्मार्टफोन अनुप्रयोगों का उपयोग करना सीखते जाते हैं, यूट्यूब वीडियो देखते हैं और बनाते हैं, ऑनलाइन डिजिटल गेम खेलते हैं, सीखने के लिए वेब-सर्च का उपयोग करते हैं और बहुत कुछ करते हैं। वे वर्तमान पीढ़ी में 'डिजिटल युग के बच्चे' हैं।

वर्तमान युग में बच्चों का पालन-पोषण इसलिए एक चुनौती है क्योंकि इस डिजिटल युग में एक अभिभावक के रूप में किसी को भी अच्छी तरह से तैयार होने की आवश्यकता है। प्रौद्योगिकी का जो प्रभाव बच्चों पर पड़ता है, उसके सकारात्मक और नकारात्मक प्रभाव की भी समझ होनी चाहिए। माता-पिता को बच्चे पर डिजिटल प्रौद्योगिकी के प्रभाव के बारे में जागरूक और सतर्क होना चाहिए। यह उन्हें डिजिटल तकनीक का उपयोग करने के लिए बच्चे को सही तरीके से मार्गदर्शित करने में सक्षम बनाता है, जो प्रगतिशील और सक्षम हो सकता है। साथ ही उन्हें डिजिटल दुनिया की संभावित आशंकाओं और खतरों से दूर रख सकता है। डिजिटल युग में पालन-पोषण में आवश्यक है कि अभिभावक नई अनुकूलित शैली के साथ बच्चों का पोषण करें, जो डिजिटल ज्ञान उनके, ज्ञान को डिजिटल रूप से सक्षम और जागरूक नागरिकों/नेटिज़न्स (इन्टरनेट पर सक्रिए लोग) की अगली पीढ़ी से जोड़ता हो।



## बच्चों में देखी जाने वाली डिजिटल आदतें और उनके प्रभाव

अलग-अलग उम्र के बच्चों में निम्नलिखित डिजिटल आदतों को देखा गया। इनके प्रभाव और अभिभावकों के लिए डिजिटल डिवाइस सुरक्षा और सुरक्षित ऑनलाइन अनुभव सुनिश्चित करने के लिए सुझाए गए उपाय।



वे सोशल मीडिया प्लेटफॉर्म पर अपनी उपस्थिति को बहुत महत्व देते हैं और दोस्तों के साथ ऑनलाइन बातचीत करते हैं।

सोशल मीडिया पर उपस्थिति बच्चों के आउटरीच, संचार और सूचना का फायदा उठा सकती है, हालांकि यहाँ सभी आयु वर्ग के बच्चों को इंटरनेट पर धमकाने, ट्रोलिंग और अन्य खतरों की संभावना है। यह गंभीर रूप से एक बच्चे को भावनात्मक और शारीरिक रूप से भी प्रभावित कर सकता है।

ऐसे परिदृश्य में बच्चों की मदद करने के लिए तैयार और जागरूक होने के अलावा, अभिभावकों को परिवार में मज़बूत और स्वस्थ संबंध का निर्माण करना चाहिए, उन्हें बच्चों को अपने ऑनलाइन मुद्दों को साझा करने और मार्गदर्शन लेने के लिए प्रोत्साहित करना चाहिए।

बच्चे अक्सर विभिन्न प्रयोजनों के लिए अभिभावकों के डेस्कटॉप/लैपटॉप/मोबाइल पर इंटरनेट का उपयोग करते हैं- जैसे कि ज्ञानवर्धन के लिए जानकारी की जाँच करना, गेम खेलना आदि।

माता-पिता के निजी उपकरणों में महत्वपूर्ण व्यक्तिगत जानकारी और संवेदनशील वित्तीय डेटा होते हैं, जिसका अनजाने में बच्चों द्वारा गलत प्रयोग किया जा सकता है, यदि उन्हें सुरक्षा खतरों के बारे में ठीक से जानकारी नहीं हो तो।

अभिभावकों को बच्चों को डिजिटल उपकरण देते समय अपनाए जाने वाले सुरक्षा उपायों के बारे में जागरूक होना चाहिए। साथ ही उन्हें बच्चों को डिजिटल उपकरणों के सही तरीके और सावधानीपूर्वक उपयोग के बारे में जागरूक करना चाहिए।





बच्चों को वीडियो देखना बहुत पसंद है और उन्हें अक्सर यूट्यूब, आदि जैसी वीडियो साझा करने वाली साइटों तक पहुँचते देखा जाता है।

ऑनलाइन वीडियो मनोरंजन और जानकारी का अच्छा स्रोत हैं, जबकि वहाँ दुर्भावनापूर्ण लिंक (malicious links) हो सकते हैं, जो यूट्यूब जैसी वीडियो साझा करने वाली साइट में बदल सकते हैं। जिसके माध्यम से धोखेबाज़ उपयोगकर्ता डिजिटल उपकरणों को हैक करना चाहिए।

अभिभावकों को ऑनलाइन होने के संभावित खतरों के प्रति बच्चों का उचित मार्गदर्शन करना चाहिए। उन्हें इन दुर्भावनापूर्ण लिंक (malicious links) जो यूट्यूब वीडियो पर पॉप अप कर सकते हैं, के बारे में पता होना चाहिए और बच्चों को डिवाइस हैक होने के खतरों के बारे में उचित रूप से जागरूक करना चाहिए।

बच्चे अपने मोबाइल फ़ोन और अन्य डिजिटल गैजेट्स पर बहुत सारे मुफ्त ऐप डाउनलोड और उपयोग करते हैं।

मुफ्त ऐप आपके डिवाइस को मैलवेयर, रैनसमवेयर से संक्रमित कर सकते हैं और सुरक्षा भय जैसे डेटा लीकेज, हैकिंग की आशंका आदि कारण बन सकते हैं।

माता-पिता को अधिकृत प्ले स्टोर से एप्लिकेशन डाउनलोड करने के महत्व से संबंधित जानकारी साझा करने में सक्षम होना चाहिए और उन्हें सुरक्षा पर खतरों और ऐप्स के उपयोग से संबंधित गोपनीयता के मुद्दों के बारे में भी सचेत रहना चाहिए।



बच्चे अपनी व्यक्तिगत जानकारी जैसे नाम, ईमेल आईडी, पता, मोबाइल नंबर, स्कूल का विवरण इत्यादि को अपने ऑनलाइन मित्रों के साथ खुले तौर पर साझा करने में झिझकते नहीं।

जबकि ऑनलाइन संचार संबंधों का निर्माण कर सकता है, व्यक्तिगत जानकारी साझा करना सुरक्षा से संबंधित खतरों को बढ़ा सकता है- जैसे पहचान की चोरी, फ़िशिंग आदि।

अभिभावकों को चाहिए कि वे बच्चों को व्यक्तिगत रूप से ऑनलाइन जानकारी साझा करने के खतरों के बारे में उचित रूप से बताएं। उन्हें बच्चों को यह बताने में सक्षम होना चाहिए कि यह कैसे पहचान की चोरी को बढ़ावा दे सकता है। इसका धोखेबाजों द्वारा दुरुपयोग किया जा सकता है।



बच्चे ऑनलाइन शॉपिंग को काफ़ी दिलचस्प मानते हैं और ऑनलाइन शॉपिंग करना पसंद करते हैं।

जबकि ऑनलाइन शॉपिंग लागत प्रभावी विकल्पों की एक विस्तृत श्रृंखला में डाल सकती है। वे कई आशंकाओं और खतरों को भी बढ़ा सकते हैं जैसे कि वित्तीय चोरी, नकली ऑफ़र, असुरक्षित/ धोखाधड़ी वाली साइटें, डेटा उल्लंघन, फ़िशिंग हमले, मैलवेयर के हमले आदि।

अभिभावकों को चाहिए कि वे बच्चों को खतरों और ऑनलाइन वित्तीय घोटालों के बारे में बताएं, जो असुरक्षित साइटों पर ऑनलाइन खरीदारी करते समय उन्हें प्रभावित कर सकते हैं। उन्हें अपने व्यक्तिगत और वित्तीय विवरणों को साझा करते समय सावधान रहने के लिए जागरूक करने की आवश्यकता है।





## अभिभावक-बच्चे के बीच मजबूत संबंध का निर्माण करना



किसी भी संबंध में पहला कदम मजबूत, स्वस्थ बंधन का निर्माण करना है। इससे बच्चे में विश्वास पैदा करने में मदद मिलेगी, इसके लिए ज़रूरी है कि उनमें आत्मविश्वास पैदा हो और मार्गदर्शन मिले।

1. **अभिभावक बच्चे के बीच मजबूत संबंध:** माता-पिता को एक ऐसा माहौल बनाने की ज़रूरत है, जहां बच्चे अपनी डिजिटल गतिविधियों के बारे में आपसे बात करने में सहज और स्वतंत्र महसूस करें। अभिभावक द्वारा अपने बच्चे के साथ संबंध के लिए निम्नलिखित उपायों पर विचार किया जा सकता है

- 📅 **गर्मजोशी, प्यार भरी बातचीत:** सुनिश्चित करें कि आपका बच्चा जानता है कि आप उनसे प्यार करते हैं, उनका समर्थन करते हैं और उन पर भरोसा करते हैं। इससे वे आपसे खुलकर बात कर पाएंगे और उन चीजों के बारे में अपनी चिंताओं को साझा कर पाएंगे, जो उन्हें ऑनलाइन परेशान करती हैं और सूचना लेना चाहती हैं।
- 📅 **गुणवत्तापूर्ण समय बिताएं और ऑनलाइन सुरक्षा मुद्दों के बारे में,** डिजिटल उपकरणों और इंटरनेट के उपयोग के बारे में बच्चों के साथ उनके ज्ञान को समझने के लिए नियमित रूप से पारिवारिक चर्चा करें। यह आपको डिजिटल उपकरण के उपयोग के प्रति मीडिया साक्षरता और स्व-नियामक कार्यों पर उनको आंकलन और मार्गदर्शित करने में मदद करेगा।
- 📅 **उनसे उनके ऑनलाइन गतिविधि पैटर्न के बारे में जानें,** जिससे आपके बच्चे को सर्वोत्तम तरीके से प्रौद्योगिकी और इंटरनेट का उपयोग करने में मदद मिल सके।

2. **सज़ा/ पुरस्कार के रूप में डिजिटल उपकरणों का उपयोग:** एक घर के माहौल को खुशहाल, मज़बूत बनाए रखने के लिए दत्तक माता-पिता के रूप में, अनुशासन और दिनचर्या महत्वपूर्ण है। लेकिन डिजिटल उपकरणों के उपयोग के साथ उनके अच्छे और बुरे व्यवहार को जोड़ना उचित नहीं है।

डिजिटल उपकरणों से पुरस्कार और दंड को अलग रखें। बच्चे जाने-अनजाने में मीडिया का उपयोग करते हुए गलतियां करते हैं। सहानुभूति के साथ इनको संभालने की कोशिश करें और गलती को एक सीखने वाले क्षण में बदल दें। अपने बच्चे के व्यवहार के लिए सज़ा और इनाम के रूप में डिजिटल उपकरणों का उपयोग न करें। उन्हें साइबर स्पेस में समस्याओं के लिए दोषी न ठहराएं, इससे उनमें डर पैदा होगा और वे चीजों को छिपाना शुरू कर सकते हैं।

ऐसे नियम/ अनुबंध बनाने पर विचार करें, जिस पर पारस्परिक रूप से सहमति हो, लेकिन याद रखें, लक्ष्य उन्हें दंडित करने का नहीं है, बल्कि स्पष्ट सीमाओं को निर्धारित करने का है।

3. **आवश्यकता पड़ने पर पेशेवर व्यक्ति से मदद लें:** अगर बच्चे में इंटरनेट की लत के मज़बूत संकेत दिखते हैं, तो माता-पिता को पेशेवर व्यक्ति से मदद लेने पर विचार करना चाहिए।

सीखें और एक साथ अन्वेषण करें: डिजिटल दुनिया का पता लगाने, सीखने और खोजने के अवसरों पर एक साथ समय बिताकर आप अपने बच्चे के उन कौशलों को विकसित करने में मदद कर सकते हैं, जिससे सुनिश्चित और सुरक्षित सीखने के माहौल की उन्हें ज़रूरत है।

उनके जानने के लिए कुछ अच्छी सामग्री का सुझाव दें और चर्चा करें। ऑनलाइन सीखने के लिए सहायक बनें। साथ ही प्रौद्योगिकी कौशल सीखने पर विचार करें।

खुले विचार रखें: अपने बच्चे को इंटरनेट की खोज के प्रति बहुत कठोर न हों और न ही अपने बच्चे के फ़ोन/ कंप्यूटर से ऑनलाइन एक्सेस को पूरी तरह से हटा दें। यह उन्हें अपने साथियों से अलग कर सकता है और उनके ऑनलाइन सीखने में बाधा डाल सकता है। बल्कि यह उन्हें सुरक्षा जागरूकता के साथ विनियमित उपयोग भी सिखाना है।

## घर में सुरक्षित वातावरण का निर्माण करें।



घर एक ऐसी जगह है जो आपको सुरक्षा और संरक्षण का एहसास कराती है। घर पर डिजिटल रूप से सुरक्षित और स्वस्थ वातावरण सुनिश्चित करने के लिए कुछ क्रियाओं के पालन करने की आवश्यकता होती है।

1. **माता-पिता की देखरेख में डिजिटल डिवाइस:** माता-पिता छोटे या बड़े बच्चों को ऑनलाइन अन्वेषण करने में मदद कर सकते हैं, साथ ही उनके अकाउंट्स (खातों) और अनुकूल उपकरणों का प्रबंधन करने में मदद कर सकते हैं। माता-पिता ऐप्स का उपयोग करके, स्क्रीन समय निर्धारित करके बच्चे की ऑनलाइन गतिविधि की निगरानी कर सकते हैं।

**डिजिटल डिवाइस का पारिवारिक संसाधन के रूप में उपयोग करें:** कंप्यूटर और डिजिटल उपकरणों को परिवार के लिए एक साझे संसाधन के रूप में देखा जाना चाहिए। घर के एक कॉमन रूम में कंप्यूटर रखने से बच्चे की ऑनलाइन गतिविधि की आसानी से निगरानी में मदद मिल सकती है।

**उचित संतुलन और प्रौद्योगिकी के उपयोग को प्रोत्साहित करने के लिए सभी परिवार के सदस्यों के साथ मीडिया उपयोग के लिए पारिवारिक समझौते बनाएं।**

- दिनचर्या, सीमाएं और दिशानिर्देश स्थापित करें।
- स्क्रीन का समय निर्धारित करें। मोबाइल, टीवी, कंप्यूटर, गेमिंग कंसोल आदि सभी के लिए डिजिटल डिवाइस में स्क्रीन समय सेट करें।

**अभिभावक नियंत्रण लागू करें:** कंप्यूटर और अन्य उपकरणों पर अभिभावक नियंत्रण सेट करें।

2. **सुरक्षा सुनिश्चित करने के लिए कदम उठाएं:** इंटरनेट का उपयोग करते समय साइबर क्राइम और डेटा ब्रीच होते हैं। आपको इसके बारे में पता होना चाहिए ताकि आपके बच्चों को चेतावनी दी जा सके।


- 📋 **अपने वाई-फ़ाई को सुरक्षित करें:** वाई-फ़ाई जांच उपकरण आपके घर के वाई-फ़ाई नेटवर्क से जुड़े हों और एक मज़बूत पासवर्ड के साथ अपने घर के वाई-फ़ाई को सुरक्षित करें।
- 📋 **आयु उपयुक्त उपयोग:** बच्चे की उम्र और परिपक्वता के आधार पर वेबसाइटों तक सीमित पहुंच सुनिश्चित करें।
- 📋 **जीपीएस को बंद करें:** एक साधारण जीपीएस प्लग-इन का उपयोग करके, एक संभावित स्टाकलर आपके अपलोड किए गए, फोटो को इंटरनेट से ले सकता है और आसानी से उस फोटो से जुड़े डेटा को पढ़ सकता है और आपके बच्चे के स्थान का पता निकाल सकता है। इसलिए, अपने डिजिटल उपकरणों में सार्वजनिक रूप से अपना स्थान साझा करने से बचें।
- 📋 अपने बच्चों को पसंदीदा साइटों और सुरक्षित साइटों तक आसानी से पहुंचने के लिए बुकमार्क/तारांकित विकल्पों का उपयोग करें।

### अपने बच्चे को शिक्षित करना



ऐसी दुनिया में जहां बच्चे डिजिटल उपकरणों के साथ बड़े होते हैं और अपने जीवन में एक अभिन्न भूमिका निभाते हैं, यह जरूरी है कि डिजिटल उपयोग की स्वस्थ अवधारणाओं को सीखने में उनकी मदद की जाए और माता-पिता इन कौशल को सीखने में महत्वपूर्ण भूमिका निभाएं। शुरुआत में आप उनके साथ रहकर उनकी लगातार मदद करते हैं और जैसे ही वे कार्य करते हैं और विश्वास हासिल करते हैं कि आप पीछे हट जाते हैं। यहां कुछ तरीके दिए गए हैं जिनसे आप बच्चों को ऑनलाइन सुरक्षा के बारे में बता सकते हैं।

1. **डिजिटल कौशल के साथ एक कदम आगे रहें:** डिजिटल दुनिया में आगे रहने और सुरक्षित रहने के लिए, आपके बच्चे को गंभीर रूप से सोचने, अवलोकन करने, विश्लेषण करने और स्मार्ट समाधान करने की ज़रूरत होगी। माता-पिता को अपने बच्चे को उचित कौशल, व्यवहार और सोच के साथ इस दुनिया को नेविगेट करने के लिए खुद न सिर्फ स्मार्ट होने की ज़रूरत है बल्कि सुरक्षित, और डिजिटल प्रौद्योगिकियों से खुश और लचीला उपयोगकर्ता होने की आवश्यकता है।

 उन्हें 'स्मार्ट' बनने में सक्षम करें जब वे निम्नलिखित पहलुओं के साथ ऑनलाइन हो


**S** – (Stay Safe-सुरक्षित रहें) - किसी से भी व्यक्तिगत जानकारी साझा न करें।

**M** – (Meetup-मिलना) - किसी ऐसे व्यक्ति से कभी न मिलें जिसे आप नहीं जानते।


**A** – (Accepting Files-फ़ाइलें स्वीकार करना) - अज्ञात फ़ाइलों, चित्रों, मेलों को कभी न खोलें और न ही डाउनलोड करें।


**R** – (Reliable-विश्वसनीय) - कार्य करने से पहले प्राप्त जानकारी की प्रामाणिकता को जाँच लें।




**T** – (Tell Someone-किसी को बताएं) - यदि आप कुछ देखते/ पढ़ते हैं जो आपको चिंतित/ असहज महसूस कराए तो विश्वसनीय वयस्क को बताएं।

 अपने बच्चे के साथ मिलकर इंटरनेट पर खोज करें और ज्ञान प्राप्त करने में मदद करने के लिए सकारात्मक और नकारात्मक दोनों पहलुओं पर चर्चा करें और सही तरीके से जवाब देने के लिए महत्वपूर्ण सोच विकसित करें।




2. **व्यक्तिगत जानकारी और गोपनीयता:** बच्चे बहुत सारी व्यक्तिगत जानकारी ऑनलाइन साझा करते हैं। बच्चों को व्यक्तिगत जानकारी साझा करने के खतरों को समझना आवश्यक है और माता-पिता को व्यक्तिगत जानकारी और गोपनीयता की रक्षा के लिए उन्हें कई तरीकों से अवगत कराने की आवश्यकता है। आपके और आपके बच्चे के लिए गोपनीयता सेटिंग्स के बारे में सीखना महत्वपूर्ण है। ऑनलाइन सुरक्षा में जागरूकता पहला कदम है।

 **व्यक्तिगत जानकारी का महत्व:** अपने बच्चे को व्यक्तिगत जानकारी के महत्व को समझाएँ और उन्हें व्यक्तिगत पहचान की जानकारी (जैसे, वास्तविक नाम, पता, स्कूल, टेलीफ़ोन नंबर, फोटो, परिवार के सदस्य के नाम) को इंटरनेट/ किसी भी ऑनलाइन माध्यम पर साझा करने से बचने के लिए कहें।

 **तस्वीरें और वीडियो साझा करना:** सेल्फ़ी संस्कृति से जुड़ी तस्वीरों और वीडियो को साझा करने की संभावित समस्याओं और संभावना पर चर्चा करें, जिनका उपयोग बाद में आपके शोषण के लिए किया जा सकता है।

- 
**पासवर्ड का महत्व:** बच्चों को अपने करीबी दोस्त के साथ भी पासवर्ड साझा न करने के लिए कहें, और विशेष रूप से सार्वजनिक स्थानों पर कंप्यूटर बंद करने से पहले हमेशा अपने खातों को बंद करें।
- 
**वित्तीय जानकारी का महत्व:** महत्वपूर्ण क्रेडिट/ डेबिट कार्ड के विवरणों को साझा न करने के लिए कहें और उन्हें मुफ्त ऑनलाइन ऑफ़र और बड़े ईनाम का दावा करने वाले, धोखेधड़ी करने वाले ईमेल के खतरों के बारे में बताएं।
- 
**उपलब्ध गोपनीयता सेटिंग्स का उपयोग करें:** विभिन्न डिजिटल उपकरणों और सोशल मीडिया प्लेटफ़ार्मों पर गोपनीयता के विकल्पों के बारे में अपने बच्चे को बताएं। पोस्ट, एप्लिकेशन और प्रोफाइल के लिए अपनी गोपनीयता सेटिंग्स की पुनः जाँच करें। इस तरह, आप यह जाँच कर सकते हैं कि कौन लोग आपके बच्चे की प्रोफाइल देखते हैं और वे वास्तव में क्या देखते हैं; और ब्राउज़र की सुरक्षा सुविधाओं को “उच्च स्तर” पर सेट करें।

3. **सोशल मीडिया के नुकसान और सुरक्षा के उपाय:** सोशल मीडिया कनेक्टिविटी बच्चों के दोस्तों के साथ चैट करना, सामाजिक रूप से नेटवर्क का उपयोग करना, तस्वीरें साझा करना, संगीत वीडियो बनाना, वीडियो अपलोड करना, गेम खेलना, चैट रूम में जाना, फ़ाइल साझा करना इत्यादि जैसे बहुत से सकारात्मक अवसर और लाभ प्रस्तुत करती है। लेकिन एक ही समय में, बच्चे सोशल मीडिया का उपयोग करते समय निम्नलिखित ऑनलाइन जोखिमों का सामना कर सकते हैं।

- 
**ऑनलाइन चैटिंग:** युवाओं को ऑनलाइन चैट से दूर रखें और पुराने नियम को लागू करने की कोशिश करें, “अजनबियों से कभी बात न करें”। बिना अनुमति के जिस व्यक्ति से आप ऑनलाइन दोस्ती करते हैं, उससे मिलने वाले खतरों पर भी चर्चा करें।
- 
**ऑनलाइन ग्रूमिंग:** ऑनलाइन ग्रूमिंग के बारे में बच्चों को बताएं और बच्चे के भरोसे को जीतने की कोशिश करने वाले अजनबियों से छिपे खतरों के बारे में बच्चों को बताएं।
- 
**साइबर बुलिंग:** साइबर बुलिंग के बारे में बच्चों के साथ चर्चा करें। उन्हें अच्छी तरह से अवगत कराना चाहिए कि ऑनलाइन उत्पीड़न गंभीर भावनात्मक मुद्दों का कारण बन सकता है, इसलिए आवश्यकता पड़ने पर उन्हें तत्काल मदद लेनी चाहिए।

4. **इंटरनेट के नकारात्मक पक्ष के बारे में बताएं:** बच्चों की जानकारी के लिए इंटरनेट एक सबसे अच्छा स्रोत है, लेकिन उन्हें इंटरनेट का उपयोग करते समय छिपे खतरों के बारे में जागरूक होने की आवश्यकता है।

- ☑ **जांच करने की आवश्यकता:** अपने बच्चे को भारी मात्रा में उपलब्ध ऑनलाइन जानकारी और जानकारी की प्रामाणिकता का मूल्यांकन करने के संभावित तरीकों के बारे में बताएं।
- ☑ **अनाधिकृत वेबसाइटों से बचें:** अनाधिकृत वेबसाइटों पर कभी न जाएँ अथवा हर वेबसाइट के लिए साइन अप न करें। कई सामाजिक नेटवर्किंग साइटों (यूट्यूब, इंस्टाग्राम, आदि) पर आयु प्रतिबंध है।
- ☑ **नुकसानदायक लिंक:** यूट्यूब, इंस्टाग्राम, जैसी वीडियो साझा करने वाली साइटों पर किशोर बच्चों को नुकसानदायक लिंक, जिनके बारे में उन्हें सचेत रहना चाहिए के बारे में आगाह करें और उन्हें बताएं कि उन लिंक पर क्लिक करने से बचें जो रोमांचक ऑफर और लाभ देते हैं।
- ☑ **जाली प्रोफ़ाइल:** सेलिब्रिटी चैट समूहों/ पृष्ठों के बारे में किशोर बच्चों को जानकारी दें। उन्हें इस बात से अवगत कराया जाना चाहिए कि हो सकता है ये सेलिब्रिटी सोशल मीडिया अकाउंट/ पेज मशहूर हस्तियों या उनके प्रशंसकों द्वारा नहीं चलाए जाते हों, और उन्हें इससे सावधान रहने की आवश्यकता है।

### डिजिटल सुरक्षा के लिए सुरक्षा सुविधाओं को सक्रिय करना



यह महत्वपूर्ण है कि जब बच्चे ऑनलाइन हों या डिजिटल उपकरणों का उपयोग कर रहे हों तो माता-पिता डिजिटल रूप से कुछ महत्वपूर्ण सुरक्षा सुविधाओं और कार्यप्रणाली को लागू और सक्षम करने के लिए जागरूक और अद्यतित हों।

### बुनियादी सुरक्षा उपाय:

- ☑ सुनिश्चित करें कि आपके डिवाइस में स्थापित सभी ऑपरेटिंग सिस्टम, जैसे ही वे खुलते हैं नवीनतम सुरक्षा अपडेट्स के साथ अपडेट हैं।
- ☑ लाइसेंस समझौते को बिना पढ़े कोई भी सॉफ्टवेयर इंस्टॉल न करें और सुनिश्चित करें कि आपके बच्चे आपके डिवाइस पर कुछ डाउनलोड या इंस्टॉल करने से पहले आपकी अनुमति मांगें।
- ☑ वेबसाइटों पर ऑनलाइन लेनदेन न करें यदि URLs <https://> में “S” नहीं है, <https://> में “S” से अभिप्राय सुरक्षा (secure) से है।
- ☑ शैक्षिक वेबसाइटों या गेमिंग साइटों पर अपने कार्ड का विवरण साझा न करें। किसी भी अज्ञात शुल्क से बचने के लिए खरीदारी के विकल्प असक्रिय करें।

### डिजिटल पालन-पोषण के लिए स्मार्ट तरीके:

- ☑ अपने इंटरनेट सेवा प्रदाता से किसी भी अभिभावक नियंत्रण उपकरण के लिए कहें। वे उपकरण की पेशकश कर सकते हैं।
- ☑ अनावश्यक वेबसाइटों पर अनुचित सामग्री से बचाव के लिए अपने बच्चे के लिए ब्राउज़रों पर फ़िल्टरिंग विकल्पों का उपयोग करें।
- ☑ माता-पिता को यह सुनिश्चित करना चाहिए कि वे अपने उपकरणों को अपनी पहुँच के बाहर न छोड़ें क्योंकि बच्चे डिवाइस खोज कर सकते हैं और उसका दुरुपयोग कर सकते हैं।
- ☑ अपने बच्चे को गेम और अन्य मीडिया डाउनलोड करने से रोकेँ जो अनाधिकृत उपयोगकर्ताओं द्वारा सिस्टम के कार्यक्रमों को नुकसान पहुंचा सकते हैं।





प्रमुख ऑनलाइन सुरक्षा खतरे क्या हैं? जिनका सामना करने की संभावना बच्चों को होती है।

साइबर सिक्योरिटी की समस्या से बच्चे उतने ही असुरक्षित हैं, जितने कि वयस्क। बच्चों के सामने आने वाले कुछ सबसे बड़े खतरे हैं- स्कैम, आइडेंटिटी पहचान की गोपनीयता, फ्री डाउनलोड डेंजरस, साइबर बुलिंग, हानिकारक साइट्स के लिंक, वायरस, अनचाहे पोर्नोग्राफी, सेक्सुअली सॉलिड आदि।



मैं अपने बच्चे के साथ ऑनलाइन सुरक्षा के बारे में कैसे बात करूँ ?

बच्चों से बात करना दोतरफ़ा संचार प्रक्रिया है, जिसमें सहानुभूति और कौशल की आवश्यकता होती है। वर्तमान डिजिटल युग में, बच्चों को बहुत सारी जानकारी से अवगत कराया जाता है जो कभी-कभी उनके लिए भारी पड़ सकती है। माता-पिता को सहायक होने और परिवार के भीतर खुली बातचीत को प्रोत्साहित करने की आवश्यकता है। माता-पिता को संभावित ऑनलाइन थ्रेट्स या खतरों के लिए आवश्यक सुरक्षा उपायों को अपनाना चाहिए। उन्हें नैतिक क्रियाओं का पालन करना चाहिए और इंटरनेट और डिजिटल उपकरणों के उपयोग के लिए सबसे अच्छी क्रियाओं का स्पष्ट खाका तैयार करना चाहिए। बच्चे को उनके ऑनलाइन मुद्दों पर चर्चा करने और मार्गदर्शन लेने के लिए प्रोत्साहित किया जाना चाहिए।



हम घर पर एक सुरक्षित और स्वस्थ डिजिटल वातावरण कैसे बनाएं?

माता-पिता को अपने बच्चों को घर पर होने पर सुरक्षित डिजिटल और इंटरनेट क्रियाओं का पालन करने की आवश्यकता होती है। उन्हें इसे एक पारिवारिक क्रिया बनाना चाहिए और भोजन के समय, अध्ययन के समय, खेलने के समय डिजिटल उपकरणों का मनोरंजन के लिए उपयोग न करने के लिए सहमत होना चाहिए, और सीमित स्क्रीन समय निर्धारित होना चाहिए। बच्चे को अकेला छोड़ने के बजाय कंप्यूटर का समय सबके साथ निर्धारित करें। उन्हें बच्चों को जागरूक करना चाहिए कि डिजिटल उपकरणों का उपयोग करना एक विशेषाधिकार है और इस ज़िम्मेदारी को देखभाल और सावधानी के साथ निभाना चाहिए। इसके अलावा, परिवार के वयस्कों को डिजिटल उपकरणों पर आवश्यक सुरक्षा सुविधाओं को सक्षम करने की आवश्यकता है जैसे सुनिश्चित करें कि वाई-फ़ाई सुरक्षित है, ताकि ऑपरेटिंग सिस्टम और सॉफ़्टवेयर के उपयोग, अद्यतन एंटीवायरस की स्थापना और मैलवेयर सुरक्षा सॉफ़्टवेयर आदि अद्यतित हों।



हम हमेशा क्यों सुनते हैं? “अपना पासवर्ड साझा न करें।”

पासवर्ड साझा करने से महत्वपूर्ण जानकारियों की ऑनलाइन चोरी हो सकती है और दूसरों के हाथों में जा सकती है। पासवर्ड साझा करने से आपका डेटा और पहचान नियंत्रण से बाहर हो सकता है। यह महत्वपूर्ण है कि पासवर्ड निजी, याद रखने में आसान और अनुमान लगाने में कठिन हों।



हम अपने मोबाइल उपकरणों की सुरक्षा कैसे करते हैं?

सबसे अच्छा तरीका एक मजबूत पासवर्ड का उपयोग करना है। हमें सावधानी बरतनी चाहिए कि हम किन ऐप्स का उपयोग करते हैं। ऐसे मोबाइल उपकरणों के लिए भी सुरक्षा ऐप्स हैं जो आपका फ़ोन गुम या चोरी हो जाने पर आपके डेटा को मिटा दे। सुनिश्चित करें कि मुफ़्त या सार्वजनिक वाई-फ़ाई संरक्षित हैं और ऑटोफ़िल चालू करने से बचें, वीपीएन (वर्चुअल प्राइवेट नेटवर्क) का उपयोग करें।



निम्नलिखित कुछ सांख्यिकीय आंकड़े इंगित करते हैं कि अच्छी संख्या में भारतीय बच्चे खुद को ऑनलाइन संलग्न कर रहे हैं।

- **इंटरनेट और मोबाइल एसोसिएशन ऑफ़ इंडिया (IAMAI)** ने 'इंडिया इंटरनेट 2019' शीर्षक से अपनी रिपोर्ट में कहा है कि भारत में 451 मिलियन इंटरनेट उपयोगकर्ता थे, भारत में 451 मिलियन मासिक सक्रिय उपयोगकर्ताओं में से 385 मिलियन 12 वर्ष से अधिक आयु के हैं और 66 मिलियन 5 से 11 वर्ष की आयु वर्ग में हैं, जो परिवार के सदस्यों के उपकरणों पर इंटरनेट का उपयोग करते हैं। इसमें कहा गया है कि भारत में दो-तिहाई इंटरनेट उपयोगकर्ता 12-29 वर्ष की आयु वर्ग के हैं।
- **बच्चों और माता-पिता द्वारा आयु अनुसार मीडिया का उपयोग:** मीडिया द्वारा 2019 यूके में किए गए अध्ययन के आधार पर मीडिया का उपयोग और दृष्टिकोण पर रिपोर्ट। यह रिपोर्ट 5-15 वर्ष की आयु के बच्चों और युवाओं के साथ-साथ 3-4 साल की उम्र के बच्चों की मीडिया तक पहुँच और मीडिया के उपयोग के बारे में, दृष्टिकोण और समझ के बारे में साक्ष्य प्रदान करती है। उनके अध्ययन का एक स्नैपशॉट नीचे दिखाया गया है।

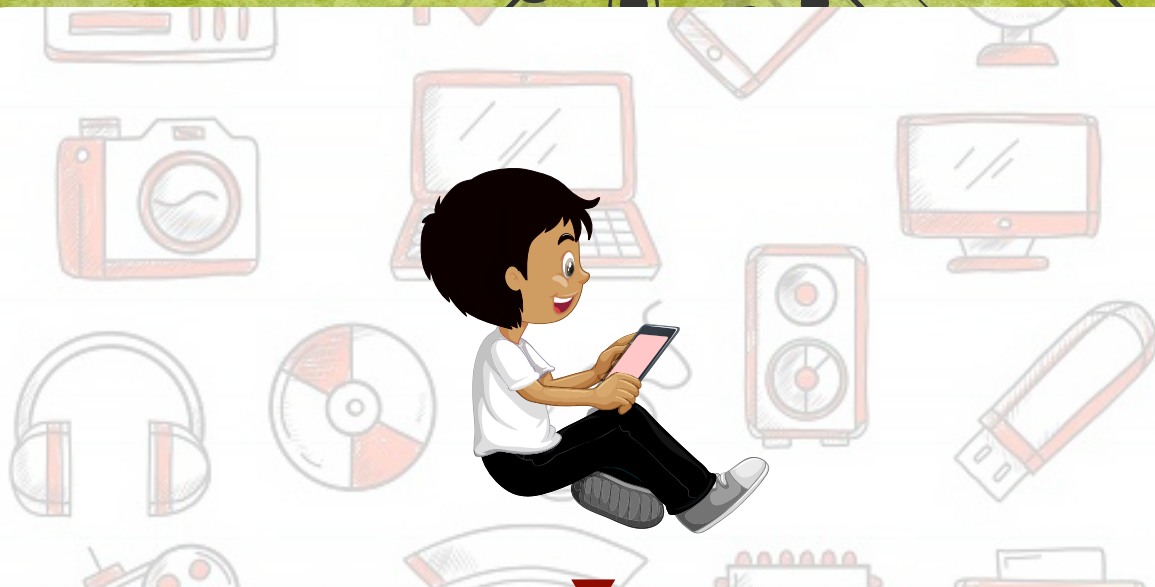


## 2019 में आयु अनुसार मीडिया का प्रयोग:



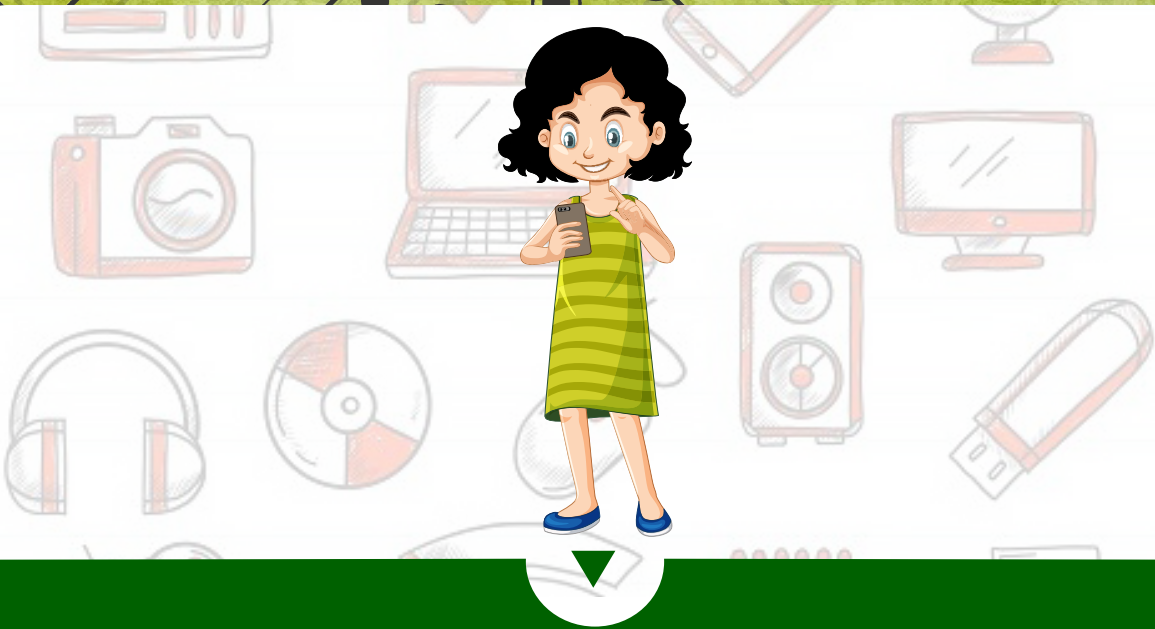
### 3-4 साल

- 24% के पास अपना टेबलेट है।
- 20% ऑनलाइन होने के लिए स्मार्ट फ़ोन का प्रयोग करते हैं।
- 15% को टेबलेट के मालिक द्वारा सोने से पहले फ़ोन दिया जाता है।
- 11% घर पर स्मार्ट स्पीकर का प्रयोग करते हैं।
- 95% टीवी देखने के लिए टीवी का, जबकि टीवी देखने के लिए 36% टेबलेट और 14% मोबाइल का प्रयोग करते हैं।
- 98% सप्ताह में 12 घंटे 42 मिनट (किसी भी उपकरण पर) फ़िल्म या टीवी प्रोग्राम देखते हैं।
- 75% लाइव प्रसारण देखते हैं और 65% वीडियो ऑन डिमांड सामग्री देखते हैं।
- 39% सप्ताह में 4 घंटे 42 मिनट गेम खेलते हैं।
- 17% ऑनलाइन गेम खेलते हैं।
- 51% सप्ताह में 8 घंटे 6 मिनट यूट्यूब देखते हैं।
- 3% यूट्यूब और ब्लॉगर्स देखते हैं।
- 1% ऑनलाइन उपयोगकर्ता का सोशल मीडिया प्रोफ़ाइल है।



## 5-7 साल

- 5% के पास अपना स्मार्ट फ़ोन है।
- 37% के पास अपना टेबलेट है।
- ऑनलाइन होने के लिए 27% स्मार्ट फ़ोन का और 63% टेबलेट प्रयोग करते हैं।
- 14% को टेबलेट के मालिक द्वारा सोने से पहले फ़ोन दिया जाता है।
- 20% घर पर स्मार्ट स्पीकर का प्रयोग करते हैं।
- 96% टीवी देखने के लिए टीवी का, जबकि टीवी देखने के लिए 40% टेबलेट और 12% मोबाइल का प्रयोग करते हैं।
- 98% सप्ताह में 11 घंटे 06 मिनट (किसी भी उपकरण पर) फिल्म या टीवी प्रोग्राम देखते हैं।
- 73% लाइव प्रसारण देखते हैं और 73% वीडियो ऑन डिमांड सामग्री देखते हैं।
- 62% सप्ताह में 6 घंटे 18 मिनट गेम खेलते हैं।
- 35% ऑनलाइन गेम खेलते हैं।
- 64% सप्ताह में 8 घंटे 36 मिनट यूट्यूब देखते हैं।
- 11% यूट्यूब और ब्लॉगर्स देखते हैं।
- 4% ऑनलाइन उपयोगकर्ता का सोशल मीडिया प्रोफ़ाइल है।




## 8-11 साल

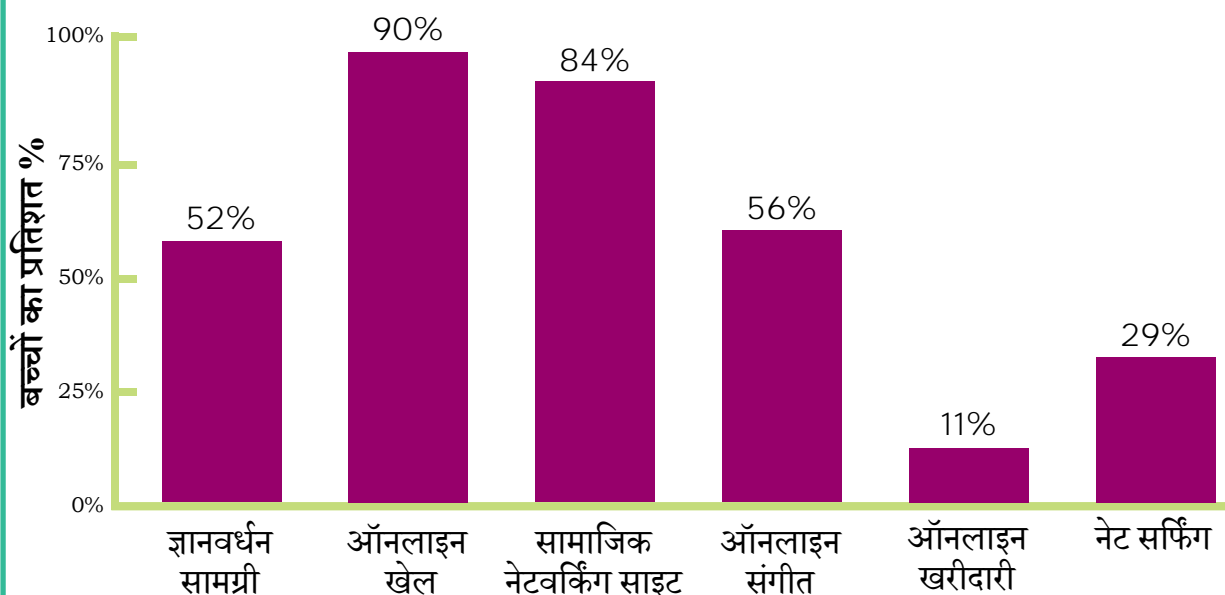
- 37% के पास अपना स्मार्ट फ़ोन है और 49% के पास अपना टेबलेट है।
- ऑनलाइन होने के लिए 49% स्मार्ट फ़ोन का और 72% टेबलेट प्रयोग करते हैं।
- 45% जो मोबाइल फोन के मालिक हैं, उन्हें इसे अपने साथ बिस्तर पर ले जाने की अनुमति है, जबकि 32% टेबलेट मालिकों को ऐसा करने की अनुमति है।
- 25% घर पर स्मार्ट स्पीकर का प्रयोग करते हैं।
- 92% टीवी देखने के लिए टीवी का, जबकि टीवी देखने के लिए 42% टेबलेट और 22% मोबाइल का प्रयोग करते हैं।
- 99% सप्ताह में 10 घंटे 30 मिनट (किसी भी उपकरण पर) फिल्म या टीवी प्रोग्राम देखते हैं।
- 74% लाइव प्रसारण देखते हैं और 78% वीडियो ऑन डिमांड सामग्री देखते हैं।
- 79% सप्ताह में 9 घंटे 30 मिनट गेम खेलते हैं।
- 66% ऑनलाइन गेम खेलते हैं।
- 74% सप्ताह में 8 घंटे यूट्यूब देखते हैं।
- 27% यूट्यूब और ब्लॉगर्स देखते हैं।
- 21% ऑनलाइन उपयोगकर्ता का सोशल मीडिया प्रोफ़ाइल है।




## 12-15 साल


- 83% के पास अपना स्मार्ट फ़ोन है और 59% के पास अपना टेबलेट है।
- ऑनलाइन होने के लिए 81% स्मार्ट फ़ोन का और 69% टेबलेट प्रयोग करते हैं।
- 74% को टेबलेट के मालिक द्वारा सोने से पहले फ़ोन दिया जाता है।
- 36% घर पर स्मार्ट स्पीकर का प्रयोग करते हैं।
- 88% टीवी देखने के लिए टीवी का, जबकि टीवी देखने के लिए 46% टेबलेट और 41% मोबाइल का प्रयोग करते हैं।
- 98% सप्ताह में 11 घंटे 48 मिनट (किसी भी उपकरण पर) फिल्म या टीवी प्रोग्राम देखते हैं।
- 75% लाइव प्रसारण देखते हैं और 88% वीडियो ऑन डिमांड सामग्री देखते हैं।
- 81% सप्ताह में 11 घंटे 36 मिनट गेम खेलते हैं।
- 72% ऑनलाइन गेम खेलते हैं।
- 89% सप्ताह में 11 घंटे यूट्यूब देखते हैं।
- 41% यूट्यूब और ब्लॉगर्स देखते हैं।
- 71% ऑनलाइन उपयोगकर्ता का सोशल मीडिया प्रोफ़ाइल है।

 दमन दीप कौर गुलाटी असिस्टेंट प्रोफेसर द्वारा प्रस्तुत शोध पत्र 'भारतीय शहरी परिवारों के बच्चों के बीच इंटरनेट उपयोग पैटर्न का एक अध्ययन' के अनुसार 90% बच्चे गेम खेलने के लिए इंटरनेट का उपयोग करते हैं और 84% सोशल नेटवर्किंग साइट्स पर जुड़ने के लिए।



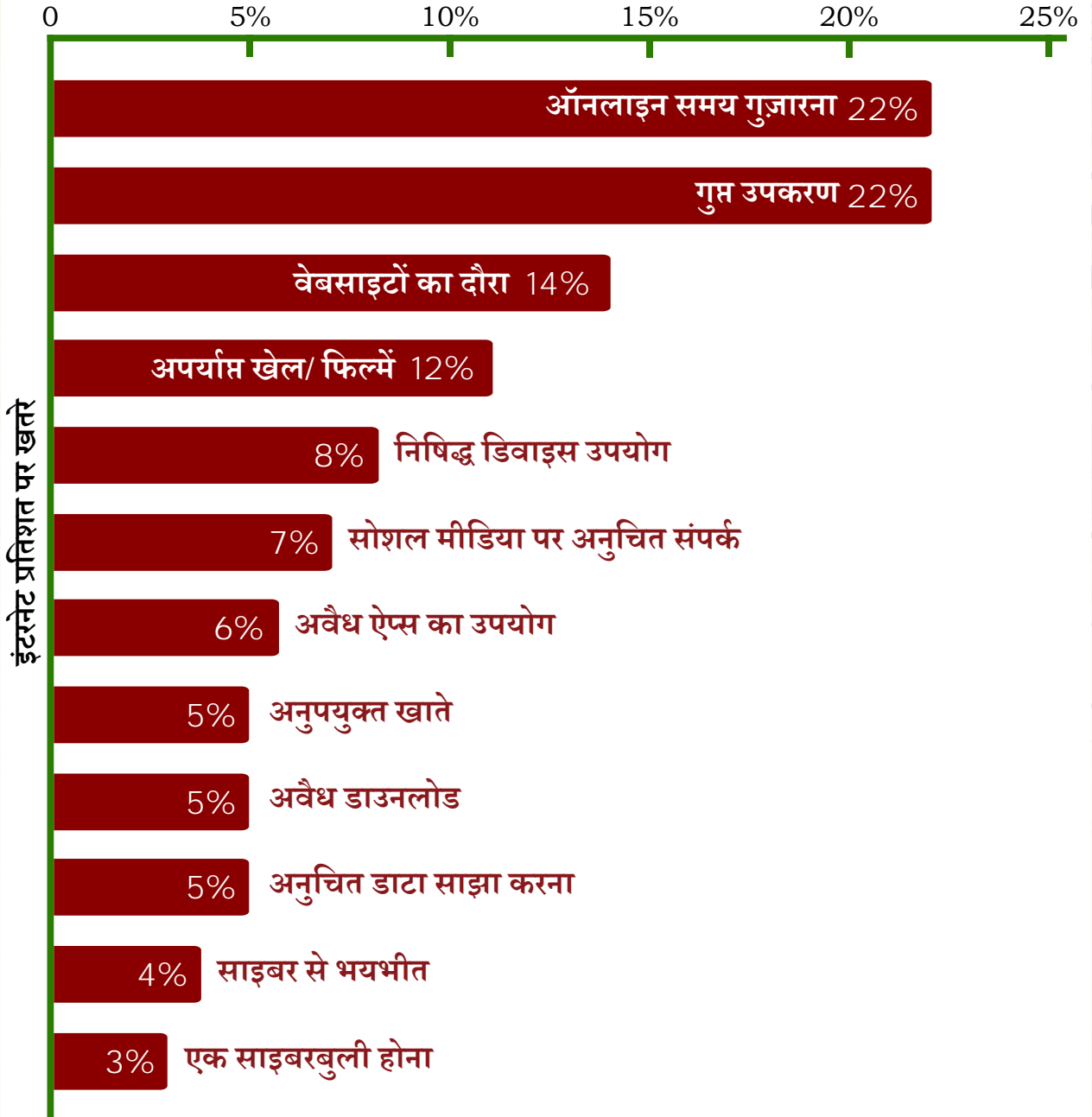
इसके अलावा, NDTV ने यह भी बताया (2017) कि शहरी भारत में नौ से सत्रह वर्ष की आयु के ज्यादातर बच्चे मोबाइल पर दिन के लगभग 4 घंटे इंटरनेट पर बिताते हैं। टेलीकॉम ऑपरेटर टेलीनॉर द्वारा जारी वेब वाइज़ के सर्वेक्षण के अनुसार, 2017 तक 134 मिलियन भारतीय बच्चों के ऑनलाइन आने का अनुमान है। मोबाइल फ़ोन बच्चों का पसंदीदा उपकरण है और उनमें से 62.4 प्रतिशत बच्चे इंटरनेट पर प्रतिदिन 4 घंटे तक व्यतीत करते हैं।

 टेलीनॉर इंडिया वेब वाइज़ की रिपोर्ट (2016) बताती है कि बच्चे हैकिंग, अनुचित संदेश प्राप्त करने, ऑनलाइन ठगे जाने आदि के प्रति बेहद संवेदनशील हैं।

 कास्परस्काई लैब रिसर्च (2016) के अनुसार: विश्व स्तर पर, गोपनीयता पर बहुत अधिक खतरे को चिह्नित किया गया है।



## प्रभावित प्रतिशत



इंटरनेट प्रतिशत पर खतरा

0101000101000010100101100110010000010100101100110010001001  
10011011011101101101010010100100000011001001100001011011001100100  
011011101101101001000000111010001100101011100001110100001000000110  
011101011101101001011011100110011001000000110111011011000100000011  
01000011001010111001001100101001000000110011001101110110010001000  
0001100110110010101110100011101000110100101101110011001100100000011  
1010001101000011001010010000001100010011010010110111001100001011100  
10011100100100000011101100110000101101100011101010110010101110011001  
000000110111011001100010000001101001011101000010111001010100011010  
0001101001011100110010000011010010111001100100000011100110110111011  
01101011001010010000001110010011000010110111001100100011011101101101  
0010000001110100011001010111100001110100001000000110011101011110110  
1001011011100110011100100000011011101101110001000000110100001100101  
011100100110010000000110011001110111011001000000011001110110110110

**ISEA कार्यशालाओं के संदर्भ:** वर्षों से ISEA देश भर में जागरूकता कार्यशालाओं और प्रतियोगिताओं के माध्यम से बच्चों के साथ बातचीत कर रही है। जिसमें यह पाया गया कि मार्च 2020 से विश्व में बड़े पैमाने पर बदलाव होने के साथ ही, एक बच्चा विभिन्न शैक्षिक, मनोरंजक, सामाजिक संपर्क, रचनात्मक कार्यों आदि के लिए प्रति सप्ताह औसतन 22 बार स्क्रीन पर समय बिताता है।

जहाँ बच्चों और माता-पिता को विभिन्न शैक्षिक और सामाजिक-आर्थिक आवश्यकताओं के लिए ऑनलाइन होना पड़ता है, वहाँ औसत स्क्रीन समय प्रति सप्ताह 48 घंटे तक बढ़ गया है।

उपरोक्त सभी आंकड़े और अनुमान उन खतरों को इंगित करते हैं जहाँ कि बच्चे ऑनलाइन जोखिमों की चपेट में हैं। यह उन पहलुओं को इंगित करता है जिन्हें मुख्य रूप से माता-पिता द्वारा संबोधित करने की आवश्यकता है जैसे- स्क्रीन समय को सीमित करना, सर्वोत्तम ऑनलाइन क्रियाओं का पालन करना, ऑनलाइन खतरों बारे में जागरूकता, सुरक्षा और सुरक्षा उपायों को अपनाने की आवश्यकता है।





आज तकनीक ने हमें एक विशाल मंच प्रदान किया है जिसमें अपार अवसर हैं। यह प्रौद्योगिकी के उपयोग के माध्यम से हैं। जो हमारे पास अपनी उंगलियों पर जानकारी है; यह हमें नई चीजों के बारे में जानने और ज्ञान प्राप्त करने में सक्षम बनाती है, जैसे पहले कभी नहीं था। यह हमें कुछ चुनौतियां भी देती है, जिनके लिए हमें आवश्यक सुरक्षा उपायों को अपनाने के लिए जागरूक होने और तैयार रहने की आवश्यकता है। हमें प्रौद्योगिकी के लाभों को समझने की आवश्यकता है जो इसके प्रस्तुत नुकसान से कहीं अधिक हैं। हम प्रौद्योगिकी के इन उत्तरोत्तर उपयोगी पहलुओं का प्रभावी ढंग से उपयोग कर सकते हैं, यदि हम अपने आप को उचित रूप से और सुरक्षित रूप से उपयोग करने के लिए सही ज्ञान, जानकारी और क्रियाओं से लैस करें।

वर्तमान डिजिटल युग में, यह आवश्यक है कि डिजिटल युग के बच्चों के माता-पिता के रूप में खुद को डिजिटल ज्ञान, अभिभावक कौशल और सुरक्षा जागरूकता के सही संयोजन से लैस करें। यह हमें इस साइबर युग के डिजिटल रूप से सक्षम नेटिजन्स के रूप में विकसित करने एवं के लिए बच्चों को उचित रूप से विकसित करने के लिए पोषण और संरक्षक दोनों में मदद करता है।

## संदर्भ

<https://www.researchgate.net/publication/332107683> A study of internet usage pattern among children of Urban Families'

<https://www.bloombergquint.com/technology/about-15-of-indias-internet-users-are-aged-5-11-years-says-iamai-report>

[https://www.ofcom.org.uk/data/assets/pdf\\_file/0023/190616/children-media-use-attitudes-2019-report.pdf](https://www.ofcom.org.uk/data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf)

<https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-to-reach-627-million-in-2019-report/articleshow/68288868.cms>

<https://www.ndtv.com/india-news/indias-urban-children-spend-4-hours-on-mobile-internet-per-day-survey-1275223>

<https://www.infosecawareness.in/>

अधिक जानकारी के लिए

.....  
[www.ncert.nic.in](http://www.ncert.nic.in)

[www.ciet.nic.in](http://www.ciet.nic.in)

[www.ictcurriculum.gov.in](http://www.ictcurriculum.gov.in)

[www.infosecawareness.in](http://www.infosecawareness.in)

[www.cyberswachhtakendra.gov.in](http://www.cyberswachhtakendra.gov.in)



.....  
केंद्रीय शैक्षिक प्रौद्योगिकी संस्थान  
राष्ट्रीय शैक्षिक अनुसंधान और प्रशिक्षण परिषद्  
श्री अरविंद मार्ग, नई दिल्ली - 110016  
.....