

# साइबर सुरक्षा

डिजिटल दुनिया में सुरक्षित रहें

डॉ. जसकरण सिंह

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी  
NCERT

# साइबर सुरक्षा क्या है?



साइबर सुरक्षा का मतलब है कंप्यूटर, मोबाइल, नेटवर्क और डेटा को डिजिटल हमलों से बचाना।

इसे ऐसे समझें — जैसे आपके घर में मजबूत ताला होता है, वैसे ही आपकी ऑनलाइन जिंदगी के लिए भी सुरक्षा जरूरी है।

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी  
NCERT

## 4.9 अरब

लोग आज ऑनलाइन हैं

## 2,200

साइबर हमले प्रतिदिन

## 95%

हमले इंसानों को निशाना बनाते हैं

# ⚠ सामान्य साइबर खतरे



## ✉ फिशिंग (Phishing)

नकली ईमेल या मैसेज जो आपसे पासवर्ड या जानकारी चुराते हैं।

## 🕵 मैलवेयर (Malware)

हानिकारक सॉफ्टवेयर जो आपके डिवाइस में छुपकर डेटा चुराता है।

## 📶 सार्वजनिक Wi-Fi हमले

हैकर एक ही नेटवर्क पर आपका डेटा चुरा सकते हैं।

## 👁 साइबर बुलिंग

तकनीक का उपयोग किसी को डराने, धमकाने या परेशान करने के लिए।

## 🔒 अकाउंट हैकिंग

कोई आपका पासवर्ड चुराकर आपके अकाउंट में घुस जाता है।

## 📱 नकली ऐप्स (App Scams)

फर्जी ऐप्स जो असली लगते हैं लेकिन जानकारी चुराते हैं।



# फिशिंग हमला कैसे पहचानें



✉ इनबॉक्स — आपका ईमेल

From: security@paypa1.com

**विषय:** 🚨 तुरंत करें: अपना अकाउंट सत्यापित करें!

प्रिय ग्राहक,

हमें संदिग्ध गतिविधि मिली है। 24 घंटे में सत्यापित न करने पर आपका अकाउंट बंद हो जाएगा।

[यहाँ क्लिक करें](#)

© PayPa1 Corp. सर्वाधिकार सुरक्षित।

## ⚠ संदिग्ध प्रेषक

'paypa1.com' — अक्षर 'l' की जगह अंक '1' है!

## ⚠ घबराहट पैदा करना

जल्दी करो + डर = बिना सोचे काम करना।

## ⚠ नकली लिंक बटन

माउस घुमाने पर बिल्कुल अलग URL दिखता है।

## ⚠ अस्पष्ट अभिवादन

'प्रिय ग्राहक' — असली कंपनी नाम लिखती है।



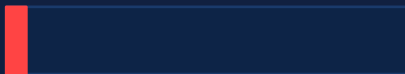
# पासवर्ड की ताकत

आपका पासवर्ड तोड़ने में कितना समय लगेगा?

password



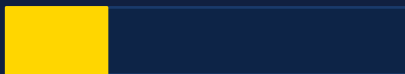
तुरंत



P@ssw0rd



कुछ मिनट



Tr0ub4dor&3



कई महीने



L!on\$Jump\*River2024



अरबों साल



## मजबूत पासवर्ड के टिप्स

- ✓ 12+ अक्षर इस्तेमाल करें
- ✓ बड़े व छोटे अक्षर मिलाएं
- ✓ नंबर और चिह्न जोड़ें
- ✓ अपना नाम या जन्मतिथि न डालें
- ✓ पासफ्रेज़ उपयोग करें
- ✓ पासवर्ड दोबारा न लगाएं
- ✓ पासवर्ड मैनेजर उपयोग करें

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी  
NCERT



# सुरक्षित सोशल मीडिया आदतें

## ✓ करें (Do)

- ✓ अकाउंट को प्राइवेट रखें
- ✓ सिर्फ जाने-पहचाने लोगों को ही जोड़ें
- ✓ पोस्ट करने से पहले सोचें — यह हमेशा के लिए है!
- ✓ मजबूत और अलग-अलग पासवर्ड रखें
- ✓ Two-Factor Authentication चालू करें
- ✓ संदिग्ध मैसेज रिपोर्ट करें

## ✗ न करें (Don't)

- ✗ अपना पूरा नाम और पता ऑनलाइन शेयर करें
- ✗ स्कूल या दिनचर्या की फोटो पोस्ट करें
- ✗ अजनबियों के लिंक पर क्लिक करें
- ✗ दोस्तों से पासवर्ड शेयर करें
- ✗ ऑनलाइन मिले अजनबी से मिलने जाएं
- ✗ धमकी भरे मैसेज का जवाब दें



# डिवाइस और नेटवर्क सुरक्षा



## डिवाइस लॉक करें

- › PIN, फिंगरप्रिंट या फेस लॉक लगाएं
- › 1 मिनट में ऑटो-लॉक सेट करें
- › डिवाइस कभी खुला न छोड़ें



## सार्वजनिक Wi-Fi के खतरे

- › पब्लिक Wi-Fi पर बैंकिंग न करें
- › VPN का उपयोग करें
- › URL में HTTPS देखें



## सॉफ्टवेयर अपडेट रखें

- › अपडेट सुरक्षा कमजोरियाँ ठीक करते हैं
- › फोन पर ऑटो-अपडेट चालू करें
- › ऐप्स को भी नियमित अपडेट करें



## सुरक्षित डाउनलोड करें

- › सिर्फ आधिकारिक ऐप स्टोर से डाउनलोड करें
- › डाउनलोड से पहले रिव्यू पढ़ें
- › कैंकड सॉफ्टवेयर से बचें



## डेटा बैकअप लें

- › हर हफ्ते क्लाउड या USB पर बैकअप लें
- › रैनसमवेयर से बचें
- › बैकअप की जांच करते रहें



## प्राइवैसी सेटिंग्स

- › ऐप परमिशन की जांच करें
- › ज्यादातर ऐप्स में लोकेशन बंद करें
- › जरूरत न हो तो Bluetooth बंद रखें



# अगर हमला हो जाए तो क्या करें?



1

**शांत रहें**

घबराएं नहीं। सोच-समझकर कदम उठाएं।

2

**इंटरनेट बंद करें**

Wi-Fi तुरंत बंद करें ताकि नुकसान न बढ़े।

3

**बड़ों को बताएं**

माता-पिता या शिक्षक को तुरंत बताएं — आप गलत नहीं हैं!

4

**पासवर्ड बदलें**

सुरक्षित डिवाइस से सभी प्रभावित अकाउंट के पासवर्ड बदलें।

5

**शिकायत दर्ज करें**

साइबर बुलिंग या हमले की स्कूल या साइबर पुलिस को रिपोर्ट करें।

6

**सबूत सहेजें**

धमकी या संदिग्ध मैसेज का स्क्रीनशॉट लें।



# आपकी साइबर हीरो चेकलिस्ट



मैं हर अकाउंट के लिए अलग मजबूत पासवर्ड रखता/रखती हूँ



मैं फिशिंग ईमेल की पहचान कर सकता/सकती हूँ



मैंने Two-Factor Authentication चालू किया हुआ है



मैं संदिग्ध लिंक पर क्लिक नहीं करता/करती



मैं अपने सॉफ्टवेयर और ऐप्स अपडेट रखता/रखती हूँ



मुझे पता है कि कुछ गलत होने पर किसे बताना है



मेरा फोन/डिवाइस ऑटोमेटिक लॉक होता है



मैं अपनी जरूरी फाइलें नियमित बैकअप लेता/लेती हूँ



मैं सोशल मीडिया पर व्यक्तिगत जानकारी शेयर नहीं करता/करती



# दो-चरण सत्यापन (Two-Factor Authentication)



## 2FA क्या है?

दो-चरण सत्यापन पासवर्ड के बाद सुरक्षा की एक और परत जोड़ता है। अगर कोई आपका पासवर्ड चुरा भी ले, तो भी वह अकाउंट में नहीं घुस सकता।

- 1 अपना यूजरनेम और पासवर्ड दर्ज करें
- 2 एक OTP कोड आपके फोन या ऐप पर आता है
- 3 कोड दर्ज करें — अब आप लॉगिन हो जाते हैं

## 2FA के प्रकार

### SMS कोड

मैसेज में आने वाला एक बार का कोड

### Authenticator ऐप

Google Authenticator जैसे ऐप से कोड मिलता है

### ईमेल कोड

आपके रजिस्टर्ड ईमेल पर कोड आता है

### बायोमेट्रिक्स

फिंगरप्रिंट या चेहरा — दूसरा चरण



# साइबर बुलिंग — क्या करें?

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी  
NCERT

साइबर बुलिंग तब होती है जब कोई टेक्नोलॉजी के जरिए किसी को परेशान करे, डराए, शर्मिंदा करे या अकेला महसूस कराए।

## ⚠ साइबर बुलिंग के संकेत

- ✗ हानिकारक या धमकी भरे मैसेज
- ✗ ऑनलाइन अफवाहें फैलाना
- ✗ शर्मनाक फोटो/वीडियो शेयर करना
- ✗ ऑनलाइन ग्रुप से बाहर करना
- ✗ किसी का नकली अकाउंट बनाना
- ✗ डॉक्सिंग — निजी जानकारी शेयर करना

## ✓ क्या करें

- ✓ जवाब मत दें और बदले की भावना छोड़ें
- ✓ सभी प्लेटफॉर्म पर बुली को ब्लॉक करें
- ✓ स्क्रीनशॉट लेकर सबूत सहेजें
- ✓ विश्वसनीय बड़े या शिक्षक को बताएं
- ✓ प्लेटफॉर्म या ऐप पर रिपोर्ट करें
- ✓ आप अकेले नहीं हैं — मदद मांगें

# AI, डीपफेक और गलत जानकारी

AI बेहद असली दिखने वाले नकली वीडियो, फोटो और टेक्स्ट बना सकता है। सावधान रहें!

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी  
NCERT

## डीपफेक वीडियो

AI से बना नकली वीडियो जिसमें किसी का चेहरा या आवाज़ बदली जाती है।

### कैसे पहचानें:

- › असामान्य पलकें झपकाना देखें
- › चेहरे के किनारे धुंधले होते हैं
- › रोशनी और रंग अजीब लगते हैं
- › मूल स्रोत से जांच करें

## AI से लिखा टेक्स्ट

नकली खबरें, समीक्षाएं या स्पैम ईमेल जो AI ने लिखे हों।

### कैसे पहचानें:

- › मूल वेबसाइट या स्रोत जांचें
- › विश्वसनीय समाचार साइटों पर देखें
- › बहुत भावुक या चरम दावों पर संदेह करें
- › फैक्ट-चेकिंग साइट्स का उपयोग करें

## AI से बनी नकली फोटो

ऐसी असली दिखने वाली फोटोज जो हकीकत में कभी नहीं हुईं।

### कैसे पहचानें:

- › हाथों की उंगलियां अजीब हों
- › पृष्ठभूमि धुंधली या दोहराई हो
- › रिवर्स इमेज सर्च करें
- › मेटाडेटा की जांच करें



# ऑनलाइन गेमिंग सुरक्षा



**3.2 अरब**

दुनिया में गेमर्स

**40%**

ऑनलाइन उत्पीड़न के शिकार

**₹8,000 Cr+**

गेमिंग घोटालों से नुकसान

## ⚠ गेमिंग के खतरे

- ✗ अजनबी जो असल जिंदगी में मिलना चाहते हैं
- ✗ चैट में स्कूल या घर का पता बताना
- ✗ गेम में घोटाले — 'फ्री स्किन के लिए पासवर्ड दो'
- ✗ अन्य खिलाड़ियों से गाली या धमकी मिलना
- ✗ माता-पिता के कार्ड से बिना बताए खरीदारी

## ✓ सुरक्षित आदतें

- ✓ गेमर टैग इस्तेमाल करें — असली नाम नहीं
- ✓ सिर्फ जाने-पहचाने लोगों को ही फ्रेंड करें
- ✓ इन-गेम रिपोर्ट टूल से टॉक्सिक खिलाड़ियों को रिपोर्ट करें
- ✓ अपने अकाउंट का पासवर्ड कभी शेयर न करें
- ✓ माता-पिता के साथ खर्च की सीमा तय करें

# ⚠ रैनसमवेयर — डिजिटल अपहरण



रैनसमवेयर एक ऐसा मैलवेयर है जो आपकी फाइलें लॉक कर देता है और उन्हें खोलने के लिए पैसे मांगता है।

रैनसमवेयर हमला कैसे होता है:

1

पीड़ित किसी हानिकारक लिंक पर क्लिक करता है

2

मैलवेयर चुपचाप डिवाइस में इंस्टॉल होता है

3

सभी फाइलें एन्क्रिप्ट (लॉक) हो जाती हैं

4

फिरौती मांगने का नोट आता है (अक्सर क्रिप्टो में)

5

पैसे देने पर भी फाइलें वापस मिलने की गारंटी नहीं!

## बचाव के तरीके:

- ✓ फाइलें नियमित रूप से बाहरी ड्राइव या क्लाउड पर बैकअप करें
- ✓ अनजान प्रेषकों के अटैचमेंट कभी न खोलें
- ✓ ऑपरेटिंग सिस्टम और एंटीवायरस अपडेट रखें
- ✓ अनौपचारिक साइटों से सॉफ्टवेयर डाउनलोड न करें

# आपका डिजिटल फुटप्रिंट

ऑनलाइन की हर गतिविधि एक निशान छोड़ती है। यह निशान कॉलेज, नौकरी और आपकी सुरक्षा को प्रभावित कर सकता है।

## सक्रिय फुटप्रिंट

- › सोशल मीडिया पर पोस्ट, कमेंट और लाइक्स
- › आपके द्वारा अपलोड की गई फोटो और वीडियो
- › भेजे गए ईमेल और मैसेज
- › लिखी गई समीक्षाएं और फोरम पोस्ट
- › जिन अकाउंट्स में आपने रजिस्टर किया

## निष्क्रिय फुटप्रिंट

- › वेबसाइटें आपकी ब्राउज़िंग ट्रैक करती हैं
- › फोन का लोकेशन डेटा एकत्र होता है
- › सर्च हिस्ट्री सर्च इंजन में सेव होती है
- › कुकीज़ आपकी पसंद याद रखती हैं
- › IP एड्रेस से आपकी जगह का पता चलता है

 याद रखें: जो चीज़ आप माता-पिता, शिक्षक या नियोक्ता को नहीं दिखाना चाहते, वह ऑनलाइन मत डालें।





# सुरक्षित ब्राउज़िंग आदतें

क्या आप सुरक्षित वेबसाइट पहचान सकते हैं?



<https://www.mybank.com/login>

HTTPS + पैडलॉक = एन्क्रिप्टेड कनेक्शन। वैध डोमेन।



<http://mybank-secure.ru/login>

HTTPS नहीं है। विदेशी संदिग्ध डोमेन (.ru)। फिशिंग की क्लासिक पहचान!



<https://amaz0n-deals.net/order>

'amazon' में 'o' की जगह '0' है। धोखे के लिए नकली डोमेन।



<https://google.com/search?q=cats>

HTTPS + मशहूर डोमेन। बिल्कुल सुरक्षित।



हमेशा HTTPS जांचें



क्लिक से पहले लिंक देखें



पॉप-अप चेतावनियों से बचें



भरोसेमंद साइटें बुकमार्क करें

# निजी जानकारी की सुरक्षा

## PII क्या होती है?

PII (Personally Identifiable Information) यानी ऐसी जानकारी जिससे आपकी पहचान हो सके। गलत हाथों में पड़ने पर यह पहचान की चोरी, धोखाधड़ी और खतरे का कारण बन सकती है।

## ऑनलाइन कभी न शेयर करें

- ✗ पूरा नाम + जन्म तिथि
- ✗ घर का पता या फोन नंबर
- ✗ स्कूल का नाम और दिनचर्या
- ✗ पासपोर्ट, आधार या ID नंबर
- ✗ बैंक अकाउंट या कार्ड विवरण
- ✗ पासवर्ड या OTP कोड

## पहचान की चोरी कैसे होती है

1

### एकत्र करना

हैकर डेटा उल्लंघन या सोशल मीडिया से आपका नाम, जन्मतिथि लेता है

2

### प्रोफाइल बनाना

कई स्रोतों की जानकारी जोड़कर आपकी पूरी प्रोफाइल बनाता है

3

### नकल करना

आपके नाम पर अकाउंट खोलता है, लोन लेता है या सामान खरीदता है

4

### नुकसान

आपका क्रेडिट स्कोर बर्बाद, कानूनी समस्याएं या डेटा बेचा जाता है

विद्यया S मृतमश्नुते



एन सी ई आर टी  
NCERT

# प्राइवैसी सेटिंग्स समझें

आपका डेटा कौन देख सकता है? यह आपकी सेटिंग्स पर निर्भर करता है।

विद्यया S मृतमश्नुते



एन सी ई आर टी  
NCERT

## Facebook / Instagram

 डिफॉल्ट रूप से सार्वजनिक — अजनबी आपकी फोटो, पोस्ट और स्थान देख सकते हैं।

✓ समाधान: 'केवल दोस्त' या 'प्राइवेट अकाउंट' सेट करें

## गेमिंग प्लेटफॉर्म

 दूसरे खिलाड़ी आपको मैसेज कर सकते हैं, आपका नाम या स्थान देख सकते हैं।

✓ समाधान: 'नाम से ढूँढें' बंद करें, केवल दोस्तों की चैट चालू करें

## लोकेशन सेवाएं

 ऐप्स आपकी हर जगह ट्रैक करते हैं — तब भी जब उपयोग में न हों।

✓ समाधान: लोकेशन 'सिर्फ उपयोग के दौरान' या बंद रखें

## सर्च इंजन

 आपकी सर्च हिस्ट्री सेव होती है और आपकी प्रोफाइल बनाने में इस्तेमाल होती है।

✓ समाधान: संवेदनशील खोज के लिए इनकॉग्निटो मोड उपयोग करें



# प्रश्नोत्तरी — अपना ज्ञान परखें!



**प्र.1: एक ईमेल आता है कि Netflix अकाउंट बंद होगा जब तक लिंक क्लिक नहीं करते। आप क्या करेंगे?**

क. तुरंत लिंक क्लिक करें    ख. सीधे Netflix वेबसाइट पर जाएं    ग. दोस्तों को लिंक भेजें

**प्र.2: इनमें से कौन सा पासवर्ड सबसे मजबूत है?**

क. password123    ख. P@ssword!    ग. T!ger\$Jump\*42

**प्र.3: ऑनलाइन मिले किसी ने स्कूल का नाम और घर का पता माँगा। आप क्या करेंगे?**

क. बता दें — वो दोस्ताना लग रहे हैं    ख. मना करें और ब्लॉक/रिपोर्ट करें    ग. सिर्फ स्कूल का नाम बताएं



# त्वरित प्रश्नोत्तरी — अपना ज्ञान परखें!

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी  
NCERT

**प्र.1: एक ईमेल आता है कि Netflix अकाउंट बंद होगा जब तक लिंक क्लिक नहीं करते। आप क्या करेंगे?**

क. तुरंत लिंक क्लिक करें    ख. सीधे Netflix वेबसाइट पर जाएं    ग. दोस्तों को लिंक भेजें

उत्तर: ख — हमेशा सीधे वेबसाइट पर जाएं, ईमेल के लिंक पर कभी क्लिक न करें।

**प्र.2: इनमें से कौन सा पासवर्ड सबसे मजबूत है?**

क. password123    ख. P@ssword!    ग. T!ger\$Jump\*42

उत्तर: ग — लंबा, बड़े-छोटे अक्षर, नंबर और चिह्न — सबसे मजबूत।

**प्र.3: ऑनलाइन मिले किसी ने स्कूल का नाम और घर का पता माँगा। आप क्या करेंगे?**

क. बता दें — वो दोस्ताना लग रहे हैं    ख. मना करें और ब्लॉक/रिपोर्ट करें    ग. सिर्फ स्कूल का नाम बताएं

उत्तर: ख — ऑनलाइन मिले अनजान लोगों से कभी भी निजी जानकारी शेयर न करें।



# साइबर स्मार्ट बनें!

क्लिक करने से पहले सोचें। अपनी डिजिटल जिंदगी की रक्षा करें।



मजबूत पासवर्ड



फिशिंग पहचानें



ऑनलाइन सुरक्षित रहें