THE ROTARY CLUB OF POONA WEST R.I.DIST 3131 INDIA

Rotary District 3131

Pune Police

सायबर सुरक्षेसाठी मार्गदर्शक पुस्तिका

BE CYBER SAFE!

सायबर सुरक्षित राहा

रोटरी क्लब ऑफ पूना वेस्ट प्रस्तुत

प्रस्तावना

इंटरनेटचा वाढता वापर लक्षात घेता, विद्यार्थ्यांना सायबर जगातील धोके ओळखणे अत्यावश्यक झाले आहे. त्याचबरोबर त्यांना चांगले 'नेटिझन्स' (सदाचरणी इंटरनेट वापरकर्ते) कसे व्हायचे हेही शिकणे गरजेचे आहे.

ही पुस्तिका आठवी आणि नववीच्या विद्यार्थ्यांसाठी तयार करण्यात आली आहे, जेणेकरून त्यांना सायबर सुरक्षिततेच्या मूलभूत गोष्टी समजून घेता येतील.
या पुस्तिकेची भाषा सोपी आहे आणि समजायला मदत करणाऱ्या क्लिप आर्टसह सजवलेली आहे, जेणेकरून विद्यार्थ्यांना विषय समजणे सोपे जाईल आणि त्यांना तो रंजकही वाटेल.

या पुस्तिकेतील विषय तीन भागांमध्ये विभागलेले आहेत.
पहिल्या भागात सायबर सुरक्षिततेच्या मूलभूत सवयींबद्दल सांगितले आहे.
दुसऱ्या भागात विविध प्रकारचे सायबर गुन्हे काय असतात याची माहिती दिली आहे.
तिसऱ्या भागात सायबर गुन्ह्यांची तक्रार कुठे आणि कशी करावी याविषयी मार्गदर्शन दिले आहे.

आम्हाला आशा आहे की ही पुस्तिका विद्यार्थ्यांना उपयुक्त आणि माहितीपूर्ण वाटेल.

रोटे. डॉ. माधुरी घाटे,

रोटरी क्लब ऑफ पूना वेस्ट

अनुक्रमणिका (S.NO)	**विषय**	PAGE NO
1.	उपकरणांची सुरक्षितता	6
2.	सुरक्षित इंटरनेट ब्राउझिंग	10
3.	ऑनलाईन खात्यांची सुरक्षा – पासवर्ड सुरक्षितता	16
4	सोशल मीडियावरील सुरक्षिततेसाठी काळजी	21
5.	ॲप्सची सुरक्षितता	25
6.	हॅकिंग	30
7.	सायबर दादागिरी (Cyber Bullying)	35
8.	गेमिंग आणि सायबर ग्रूमिंग	40
9.	कृत्रिम बुद्धिमत्ता (AI) ची आव्हाने	44
10.	इंटरनेटचे व्यसन, सायबर फूटप्रिंट	47

11.	मूलभूत ऑनलाईन आर्थिक सुरक्षितता	52
12.	तक्रार नोंदवण्याचे माध्यम (Reporting Channels)	56

उपकरणांची सुरक्षितता
Device Safety

उपकरणांची सुरक्षितता

तुमचा फोन, टॅबलेट किंवा लॅपटॉप म्हणजे तुमची डिजिटल वही आहे.
जशी तुम्ही तुमची पुस्तके आणि दप्तर सुरक्षित ठेवता,
तशी तुम्ही तुमची उपकरणं सुद्धा सुरक्षित ठेवली पाहिजेत.

🛡️ 1. शक्तिशाली पासवर्ड किंवा लॉक स्क्रीन वापरा

✅ नेहमी **शक्तिशाली** पासवर्ड, पिन, पॅटर्न किंवा फिंगरप्रिंट वापरून
तुम चे डिव्हाइस अनलॉक करा.

❌ 1234 किंवा स्वतः चे नाव असे सोपे पासवर्ड वापरू नका

🌐 2. फक्त सुरक्षित Wi-Fi ला कनेक्ट व्हा

✅ फक्त ओळखीचं आणि विश्वासार्ह Wi-Fi (जसं की घरचे Wi-Fi) वापरा.
❌ सार्वजनिक ठिकाणी मोफत Wi-Fi ला कनेक्ट करु नका—
ते सुरक्षित नसू शकतात.

🔄 3. तुमचे डिव्हाइस नियमितपणे अपडेट करा

🔁 अपडेट्स बग्स सुधारतात आणि हॅकर्सपासून तुमचे डिव्हाइस सुरक्षित ठेवतात.

✅ नेहमी सॉफ्टवेअर अपडेट्ससाठी परवानगी द्या.

🧽 4. अज्ञात ॲप्स किंवा गेम्स डाउनलोड करू नका

✅ फक्त अधिकृत ॲप स्टोअरमधून (Google Play Store किंवा Apple App Store) ॲप्स डाउनलोड करा.
❌ अज्ञात ॲप्समध्ये व्हायरस असू शकतो किंवा ते तुमचा डेटा चोरेल.

🧼 5. अँटीव्हायरस किंवा सुरक्षा ॲप.

तुमचे डिव्हाइस व्हायरस किंवा हॅकिंगपासून वाचवण्यासाठी चांगलं अँटीव्हायरस ॲप इंस्टॉल करा.

📷 6. वापरत नसताना वेबकॅम झाका

कधी कधी हॅकर्स तुमचा वेबकॅम गुपचूप चालू करू शकतात.
✅ वापरत नसताना तो झाकलेला ठेवा.

📁 7. तुमचा डेटा बॅकअप घ्या

💾 तुमचे महत्वाचे फोटो, फायली, किंवा नोट्स Google Drive मध्ये किंवा USB मध्ये जतन करा.
त्यामुळे डिव्हाइस खराब झाल्यास किंवा हॅक झाल्यास, तुमचा डेटा सुरक्षित राहील.

🔌 8. सार्वजनिक ठिकाणी फोन चार्ज करू नका

⚠️ मॉल्स, बसमध्ये असलेल्या सार्वजनिक USB चार्जिंग पोर्ट्सचा वापर टाळा.
ते असुरक्षित असू शकतात आणि तुमचा डेटा चोरू शकतात

👦🏫 9. काही विचित्र वाटल्यास मदतीसाठी विचारा

जर तुमचं डिव्हाइस:

- अजब वागू लागलं
- अचानक संथ झालं
- विचित्र पॉप-अप्स किंवा अज्ञात ॲप्स दिसू लागले

✅ तर लगेच पालक, शिक्षक किंवा विश्वासार्ह व्यक्तींचा सल्ला घ्या.

📢 चतुर बना, सुरक्षित राहा, सायबर-सुरक्षित राहा!

तुमचे डिव्हाइस स्मार्ट आहे—तुम्ही त्याहून स्मार्ट व्हा!

सुरक्षित इंटरनेट ब्राउझिंग
SAFE INTERNET BROWSING

🔐 सुरक्षित इंटरनेट ब्राउझिंग

१. सुरक्षित आणि असुरक्षित वेबसाईट्स
२. मटेरियल डाऊनलोड करणे
३. कुकीजचा वापर
४. लिंक्सवर क्लिक करणे
५. अपडेटेड ब्राउझरचा वापर
६. VPN आणि इन्कॉग्निटो मोड

🛡️ सुरक्षित व असुरक्षित वेबसाइट ओळखण्याचे मार्ग

🔒 १. HTTPS आणि पॅडलॉक तपासा

- **सुरक्षित वेबसाइट**: https:// ने सुरू होते आणि ॲड्रेस बारमध्ये लॉकचे चिन्ह दिसते.
- **असुरक्षित वेबसाइट**: http:// ("s" शिवाय) आणि लॉक नाही.
  उदाहरणार्थ : https://www.amazon.in सुरक्षित आहे.
  http://example.com असुरक्षित आहे.

🧭 २. डोमेन नाव तपासा

- **खऱ्या साइट्स**: .com, .in, .org यांसारखे सामान्य डोमेन वापरतात.
- **फसवणूक करणाऱ्या साइट्स**: चुकीची स्पेलिंग किंवा अजब अक्षरे असतात (जसे amaz0n.com).

३. संपर्क माहिती तपासा

- **विश्वासार्ह साइट्स**: पत्ता, फोन नंबर व ईमेल स्पष्ट देतात.
- **फेक साइट्स**: संपर्क माहितीच नसते किंवा खोटी असते.

४. स्पेलिंग व डिझाइनकडे लक्ष द्या

- **खऱ्या वेबसाइट्स**: व्यावसायिक डिझाइन आणि बरोबर स्पेलिंग.
- **फेक वेबसाइट्स**: स्पेलिंगच्या चुका, अजब फॉन्ट किंवा चिन्हे असतात.

५. ब्राउझर वरील सुरक्षा विषयक सूचना वापरा

- **नवीन ब्राउझर्स**: फिशिंग किंवा धोकादायक साइट्सबाबत इशारा देतात. या इशाऱ्यांकडे दुर्लक्ष करू नका.

६. डाऊनलोड करताना सावधगिरी बाळगा

- **सुरक्षित डाऊनलोड**: विश्वासार्ह वेबसाइटवरूनच डाउनलोड करा.
- **असुरक्षित डाऊनलोड**: अज्ञात लिंक्सवर क्लिक करू नका.

७. बनावट वेबसाइट्सपासून सावध रहा

- **AI वापरून बनवलेल्या फेक साइट्स** खऱ्या सारख्या दिसू शकतात.
- **टीप**: URL काळजीपूर्वक तपासा आणि विश्वासार्हतेची चिन्हं शोधा.

🍪 कुकीज समजून घ्या

कुकीज म्हणजे आपल्या डिव्हाइसमध्ये साठवले जाणारे छोटे फाइल्स असतात जे वेबसाइट्सना तुमच्या पसंती लक्षात ठेवण्यास मदत करतात.

- **सुरक्षित वापर**: बहुतांश वेबसाइट्स अनुभव सुधारण्यासाठी कुकीज वापरतात.
- **व्यवस्थापन**: ब्राउझर सेटिंग्जमधून कुकीज हटवा किंवा मर्यादित करा.
- **गोपनीयता टीप**: अज्ञात वेबसाइट्सकडून कुकीज स्विकारताना काळजी घ्या.

📥 मटेरियल सुरक्षितपणे डाऊनलोड कसे करावे?

1. **सुरक्षित वेबसाइट वापरा**: https:// असलेलीच वेबसाइट वापरा.
2. **क्रेडिट द्या**: मटेरियल वापरताना मूळ स्त्रोताचा उल्लेख करा.
3. **थर्ड-पार्टी ॲप्स टाळा**: अज्ञात स्त्रोतांमधून ॲप्स डाउनलोड करू नका.
4. **ब्राउझर चेतावणी लक्षात घ्या**: सिक्युरिटी अलर्टकडे दुर्लक्ष करू नका.
5. **संशयास्पद लिंक्स टाळा**: सॉफ्टवेअर डाउनलोडसाठी अनोळखी लिंक्सवर क्लिक करू नका.
6. **नवीन ब्राउझर डाउनलोड करताना तपासणी करा**: वेबसाइट नवीन ब्राउझर मागत असेल, तर तो खरा आहे का ते तपासा.

🌐 VPN वापरण्याचे फायदे

VPN म्हणजे तुमच्या इंटरनेट कनेक्शनला एन्क्रिप्ट करतो आणि गोपनियता वाढवतो.

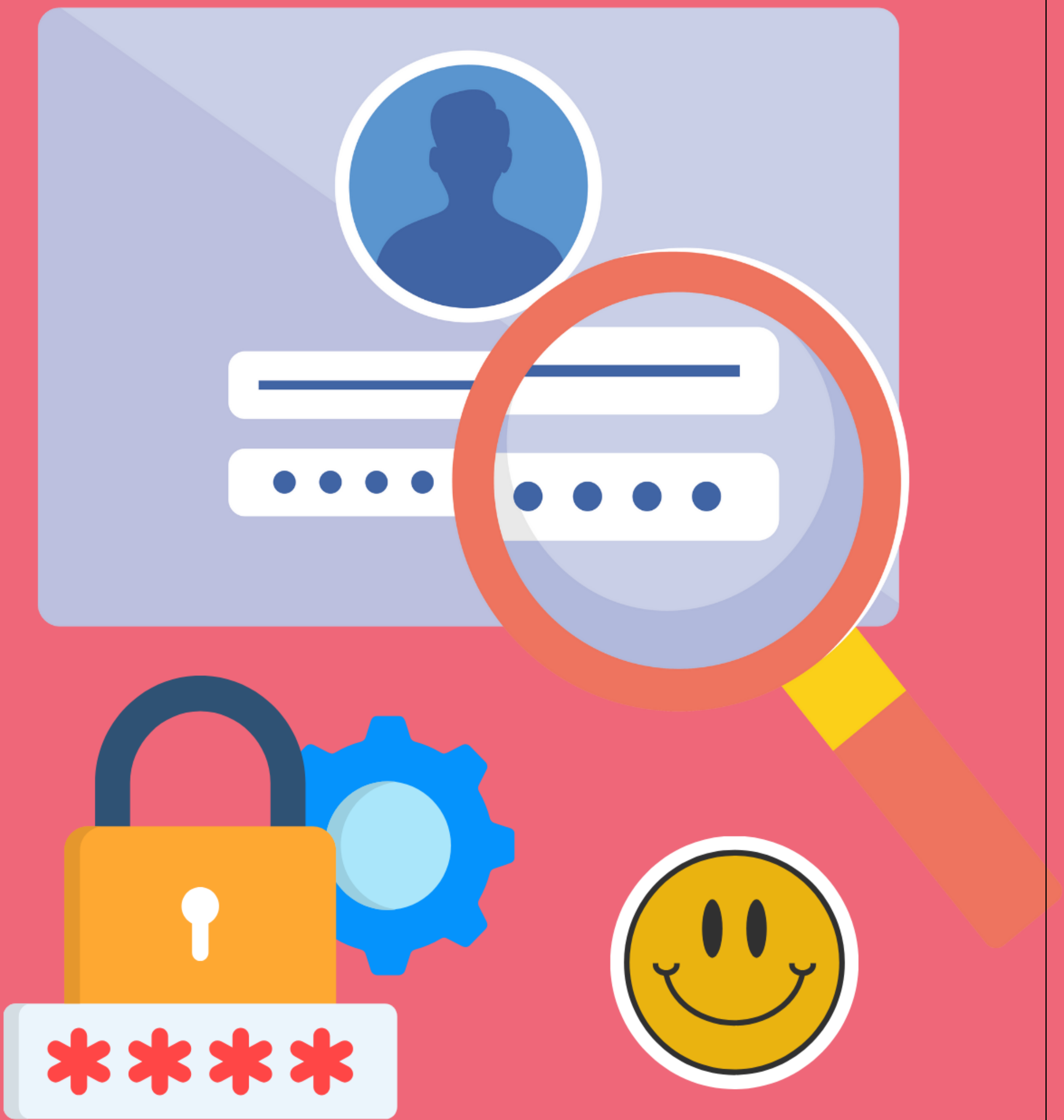
- **फायदे**: IP अ‍ॅड्रेस लपवतो, तुमचे ऑनलाइन वर्तन ट्रॅक होऊ देत नाही.
- **उपयोग**: पब्लिक Wi-Fi वर सुरक्षित ब्राउझिंगसाठी उत्तम.

🕵️ इन्कॉग्निटो मोड म्हणजे काय?

इन्कॉग्निटो मोडमध्ये ब्राउझिंग केल्यावर तुमची हिस्ट्री, कुकीज, साइट डेटा सेव्ह होत नाही.

- **काम कसे करते**: तुमचे लोकल ब्राउझिंग डेटा साठवत नाही.
- **मर्यादा**: वेबसाइट्स, इंटरनेट सर्विस प्रोव्हायडर किंवा नोकरीच्या ठिकाणी तुमचे वर्तन दिसू शकते.
- **कधी वापरावे**: शेअर्ड डिव्हाइसमध्ये प्रायव्हेट ब्राउझिंगसाठी योग्य.

ऑनलाईन खात्यांची सुरक्षा – पासवर्ड सुरक्षितता
PASSWORD SAFETY



🌐 ऑनलाइन खात्यांची सुरक्षा

१. खात्यांसाठी आणि डिव्हाइसेससाठी शक्तिशाली पासवर्ड तयार करणे
२. पासवर्डऐवजी पासफ्रेज़ वापरणे
३. पासवर्ड सुरक्षिततेसाठी नियम
४. पासवर्ड मॅनेजरचा वापर
५. टू-फॅक्टर ऑथेंटिकेशन किंवा मल्टी-फॅक्टर ऑथेंटिकेशन

🔐 पासवर्ड का महत्त्वाचे आहेत?

पासवर्ड म्हणजे तुमच्या ऑनलाइन खात्यांचा आणि उपकरणां ची **किल्ली** असते .
जर कुणी तुमचा पासवर्ड ओळखला, तर तो तुमची **खाजगी माहिती** पाहू शकतो.
म्हणूनच, तुमची खाती सुरक्षित ठेवण्यासाठी **शक्तिशाली पासवर्ड** तयार करणे गरजेचे आहे.

✅ शक्तिशाली पासवर्ड कसा तयार करावा?

1. **किमान १२ अक्षरे वापरा** – जितका पासवर्ड लांब, तितका सुरक्षित.
2. **अक्षरांचा संमिश्र वापर करा** – मोठी अक्षरे (A–Z), लहान अक्षरे (a–z), अंक (0–9) आणि खास चिन्हे (!, @, #, $, इ.).
3. **व्यक्तिगत माहिती टाळा** – तुमचं नाव, वाढदिवस, मोबाईल नंबर किंवा पाळीव प्राण्याचे नाव वापरू नका.

4. **अंदाज लावता येणार नाही असा** पासवर्ड **बनवा** – जास्त अनपेक्षित, तितका चांगला.

📝 पासफ्रेज़ म्हणजे काय?

पासफ्रेज़ म्हणजे अनेक शब्द एकत्र करून तयार केलेली ओळ.
हा पासवर्डपेक्षा **लांब आणि सुरक्षित** असतो.
उदाहरणार्थ: तुम्हाला २०२३ मध्ये गोवा ट्रिप आवडली असेल, तर पासफ्रेझ असं असू शकतो –
Holiday@Goa2023
हा लक्षात ठेवायला सोपा पण दुसऱ्यांना ओळखायला कठीण.

🛡️ पासवर्ड सुरक्षिततेचे नियम

1. **प्रत्येक खात्यासाठी वेगळा पासवर्ड वापरा** – एकाच पासवर्डचा पुनर्वापर करू नका.
2. **पासवर्ड शेअर करू नका** – गोपनीय ठेवा.
3. **पासवर्ड नियमितपणे बदला** – दर काही महिन्यांनी अपडेट करा.
4. **पासवर्ड ब्राउझरमध्ये किंवा फोनमध्ये सेव्ह करू नका** – लक्षात ठेवा किंवा पासवर्ड मॅनेजर वापरा.

🧰 पासवर्ड मॅनेजर

पासवर्ड मॅनेजरहे एक साधन आहे जे तुमचे सर्व पासवर्ड **सुरक्षितपणे साठवतो**.

तुम्हाला फक्त एक "मास्टर पासवर्ड" लक्षात ठेवावा लागतो.
📝 **टीप**: मास्टर पासवर्ड नेहमी **शक्तिशाली आणि सुरक्षित** ठेवा.

🔐 टू-फॅक्टर ऑथेंटिकेशन (2FA)

2FA म्हणजे सुरक्षा वाढवण्यासाठी **अतिरिक्त स्तर**.
तुमचा पासवर्ड माहिती असला तरी दुसरा टप्पा नसेल तर खात्यात प्रवेश होणार नाही.
उदाहरणार्थ: पासवर्ड टाकल्यानंतर तुमच्या मोबाईलवर एक कोड येतो, तो टाकल्याशिवाय लॉगिन होत नाही.

🕵️ तुमची माहिती लीक झाली आहे का? तपासा

[Have I Been Pwned] या वेबसाइटवर जाऊन तुमचा ईमेल किंवा पासवर्ड डेटा लीकमध्ये आला आहे का ते तपासा.

📚 पासवर्ड लक्षात ठेवण्यासाठी टिप्स

- **पासवर्ड मॅनेजर वापरा** – सर्व पासवर्ड सुरक्षितपणे साठवतो.
- **लक्षात राहणारी पासफ्रेझ तयार करा** – तुमच्यासाठी अर्थपूर्ण असलेले शब्द वापरा.
- **लिहून ठेवा पण सुरक्षित ठिकाणी** – लिहायचे असेल तर कुणालाही न दिसेल अशा ठिकाणी ठेवा.

📌 संक्षिप्त पुनरावलोकन

• **शक्तिशाली पासवर्ड** – किमान १२ अक्षरे, विविध प्रकारचे अक्षर व चिन्हांचा समावेश.
• **पासफ्रेझ** – लक्षात राहणारी, पण ओळखायला कठीण अशी वाक्यरचना.
• **2FA** – खात्याला अतिरिक्त सुरक्षा.
• **पासवर्ड मॅनेजर** – पासवर्ड साठवण्यासाठी आणि व्यवस्थापनासाठी सुरक्षित साधन.

सोशल मीडियावरील सुरक्षिततेसाठी काळजी
SOCIAL MEDIA SAFETY

🌐 सोशल मिडिया

१. सोशल मिडिया म्हणजे काय?
२. फ्रेंड रिक्वेस्ट हाताळणे
३. प्रायव्हसी सेटिंग्ज
४. सोशल मिडिया अकाउंट हॅक होणे
५. अयोग्य कंटेंट
६. बनावट अकाउंट ओळखणे

📱 सोशल मिडिया म्हणजे काय?

सोशल मिडिया म्हणजे इंटरनेटवरची एक जागा जिथे लोक:
- एकमेकांशी संवाद साधतात
- कल्पना, विचार, फोटो, व्हिडिओ शेअर करतात
- नवीन मित्र बनवतात
- स्वतःचा व्यवसाय किंवा वैयक्तिक ब्रँड तयार करतात

लोकप्रिय सोशल मिडिया ॲप्स:
- Facebook
- Twitter
- Instagram
- WhatsApp
- Snapchat
- Tinder

🛡️ सोशल मिडियावर सुरक्षित कसे राहायचे?

1. ❌ **अनोळखी लोकांच्या फ्रेंड रिक्वेस्ट स्विकारु नका.**
   प्रत्यक्षात ओळख असलेल्या लोकांशीच संवाद साधा.
2. 🔒 **वैयक्तिक माहिती खाजगी ठेवा.**
   तुमच्या खालील गोष्टी पोस्ट करू नका:
   o फोटो किंवा व्हिडिओ
   o घरचा पत्ता किंवा मोबाईल नंबर
   o जन्मतारीख किंवा प्रवासाची माहिती
3. 🧠 **शक्तिशाली पासवर्ड वापरा.**
   अतिरिक्त सुरक्षेसाठी टू-फॅक्टर ऑथेंटिकेशन (2FA) वापरा.
4. 📵 **ॲप्स वापरताना सावधगिरी बाळगा.**
   सोशल मिडियावरून अनोळखी ॲप्स डाउनलोड करू नका.

🔒 प्रायव्हसी सेटिंग्ज

अनेक सोशल मिडिया प्लॅटफॉर्म्सवर पालक व मुलांसाठी सेफ्टी सेटिंग्ज असतात.
त्या वापरा आणि सुरक्षित रहा.

🚫 अयोग्य कंटेंट

1. उद्धट किंवा अपमानास्पद पोस्ट्स रिपोर्ट करा.
2. फेक न्यूज किंवा न तपासलेले मेसेजेस शेअर करू नका.
3. AI ने बनवलेले फोटो किंवा व्हिडिओ नीट तपासा – सर्व काही खरं नसतं!
4. धार्मिक किंवा राजकीय भावना दुखावणारा कंटेंट फॉरवर्ड करू नका.

5. सोशल मिडियावर नम्र आणि सभ्य राहा.
6. तुमचा सोशल मिडिया हा तुमचा **डिजिटल फूटप्रिंट** आहे – कॉलेजेस व नोकरी देणारे ते तपासत असतात.

👦💻 तुमचं अकाउंट हॅक झालं तर काय कराल?

1. 🔑 लगेच पासवर्ड बदला.
2. 📧 ईमेलचा पासवर्डही बदला.
3. 📢 मित्रांना सांगा की तुमचा अकाउंट हॅक झाला आहे.
4. ⚠️ त्यांना विचित्र मेसेजेसवर क्लिक करू नका असे सांगा.
5. 🛠️ संबंधित ॲपच्या "Help Centre" चा वापर करून अकाउंट परत मिळवा.

🕵️ बनावट अकाउंट कसे ओळखावे?

1. बायो किंवा प्रोफाइल फोटो नसतो.
2. नवीन अकाउंट, ज्यावर फार कमी पोस्ट्स असतात.
3. बरेच लोक फॉलो करतो, पण त्याचे फॉलोअर्स फारच कमी असतात.
4. फेक ऑफर्स देऊन फसवण्याचा प्रयत्न करतो.
5. प्रोफाइल फोटो चोरीचा आहे का, हे तपासण्यासाठी **Google Images** वापरा.

ॲप्सची सुरक्षितता
APP SAFETY

📱 ॲप सुरक्षा (App Safety)

१. ॲप डाउनलोड करताना लक्षात ठेवण्याच्या गोष्टी
२. ॲप परवानग्या (Permissions) व लोकेशन सेवा हाताळणे
३. ॲप अपडेट करणे
४. न वापरलेले ॲप डिलीट करणे

📲 ॲप म्हणजे काय?

"**ॲप**" म्हणजे "ॲप्लिकेशन" याचे संक्षिप्त रूप आहे.
हे एक छोटे सॉफ्टवेअर असते जे तुमच्या मोबाईल, संगणक किंवा टॅब्लेटवर चालते.

ॲप्स तुमचं रोजचं काम सोपं करतात, जसं की:
• मित्रांशी चॅट करणे (WhatsApp)
• व्हिडिओ पाहणे (YouTube)
• अभ्यास करणे (Google Classroom)
• गेम्स खेळणे
• ऑफिसचे काम करणे

⚠️ ॲप डाउनलोड करण्याआधी विचार करा

डाउनलोड करण्याआधी खालील गोष्टी तपासा:

1. ✅ **फक्त Google Play Store किंवा iPhone App Store वरूनच ॲप डाउनलोड करा.**
   ❌ अनोळखी वेबसाइट्सवरून ॲप डाउनलोड करू नका.

2. ⭐ **ॲपचे रेटिंग तपासा.**
   खूप जास्त 1-स्टार किंवा 5-स्टार असतील तर फेक रिव्ह्यू असू शकतात.
3. 📈 **डाऊनलोडची संख्या तपासा.**
   जास्त डाऊनलोड्स म्हणजे ॲप अधिक विश्वासार्ह आहे.
4. 💬 **वेगवेगळ्या वेबसाइट्सवर रिव्ह्यू वाचा.**
5. 🗒 **ॲप तयार करणाऱ्या कंपनीची (vendor) माहिती तपासा.**
6. 📁 **APK फाइल्स (Android साठी)** – फक्त सुरक्षित वेबसाइट्सवरूनच डाउनलोड करा.

🔒 ॲप परवानग्या (Permissions) हाताळा

ॲप्स अनेक वेळा खालील परवानग्या मागतात:
- 📍 तुमचे लोकेशन
- 📷 कॅमेरा
- 🎤 माईक्रोफोन

➡ फक्त आवश्यक परवानग्याच द्या.
उदा. फोटो एडिटरला कॅमेरा लागेल, पण लोकेशन नाही!

➡ सेटिंग्जमध्ये जाऊन प्रत्येक ॲपने काय परवानगी घेतली आहे हे तपासा.
कधीही permissions बंद करता येतात.

🔄 ॲप अपडेट करणे

📢 फोनवर “Update Available” दिसल्यावर दुर्लक्ष करू नका!

ॲप अपडेट केल्याने:
• बग्स (तांत्रिक त्रुटी) सुधारल्या जातात
• नवीन फिचर्स मिळतात
• ॲप अधिक चांगले चालते

🗑️ न वापरलेले ॲप्स डिलीट करा

जर तुम्ही एखादे ॲप ३ महिने वापरले नसेल, तर ते डिलीट करा.

✅ ॲप डिलीट करताना ह्या पद्धतीने करा:

1. **ॲप अनइंस्टॉल करा**
   - iPhone: ॲप दाबून ठेवा → ❌ Remove App
   - Android: ॲप दाबून ठेवा → 🗑️ Uninstall
   - किंवा: Settings > Apps > [App Name] > Uninstall
2. **महत्त्वाचा डेटा बॅकअप घ्या**
   - नोट्स, फोटो, फाइल्स सेव्ह करा
   - क्लाऊडवर डेटा सिंक आहे याची खात्री करा
3. **Accounts Unlink करा**
   - सोशल मिडिया किंवा ईमेल लिंक काढा
   - सेव्ह केलेले पेमेंट मेथड्स डिलीट करा
4. **App Data साफ करा**
   - Settings → Clear cache आणि Clear data
   - यामुळे उरलेल्या फाईल्स डिलीट होतात
5. **Permissions रद्द करा**
   - कॅमेरा, कॉन्टॅक्ट्स, लोकेशन यांचा ऍक्सेस काढून टाका

6. **फोनची सुरक्षा तपासा**
   - ॲप डिलीट केल्यानंतर फोन व्यवस्थित चालतोय का ते बघा
   - काही विचित्र घडलं तर तज्ज्ञांकडून तपासणी करा !

हॅकिंग
HACKING

🔐 सायबर गुन्ह्यांपासून संरक्षण

१. हॅकिंग म्हणजे काय?
२. फिशिंग, विशिंग आणि स्मिशिंग हल्ले
३. मालवेअर हल्ल्याची लक्षणं
४. अकाउंट हॅक झाल्यास काय करावे

👦💻 हॅकिंग म्हणजे काय?

हॅकिंग म्हणजे कोणत्याही संगणक किंवा फोन सिस्टिममध्ये बेकायदेशीरपणे घुसून माहिती चोरणे किंवा हानी पोहचवणे.

🛑 घडलेली घटना:
लोकांना खोटे मेसेज आले की त्यांचे MNGL गॅस बिल थकीत आहे.
त्यामध्ये एक लिंक होती – पैसे भरण्यासाठी किंवा अॅप डाउनलोड करण्यासाठी.
ही एक फसवणूक होती, जिचा उद्देश पैसे चोरणे होता.

🎣 फिशिंग, ☎️ विशिंग आणि 💬 स्मिशिंग

🎣 फिशिंग:

• खोटे ईमेल किंवा मेसेज जे खरे वाटतात
• तुमचा पासवर्ड, ATM PIN, किंवा खासगी माहिती विचारतात
• अशा लिंक्सवर कधीही क्लिक करू नका

☎️ विशिंग:

• फसवे फोन कॉल्स – बँक किंवा सरकारी कर्मचाऱ्याचे नाटक
• तुमचे बँक तपशील विचारतात
• PIN किंवा OTP कधीही सांगू नका

💬 स्मिशिंग:

• खोटा SMS जो अतिशय तातडीचा वाटतो
• लिंकवर क्लिक करायला सांगतो किंवा माहिती मागतो
• क्लिक करू नका – मेसेज डिलीट करा

🦠 मालवेअरपासून संरक्षण कसे करावे?

मालवेअर हे एक वाईट सॉफ्टवेअर आहे जे:
• तुमची माहिती चोरू शकते
• डिव्हाइस खराब करू शकते
• तुमच्या खात्यातून स्पॅम पाठवू शकते

✅ सुरक्षित राहण्यासाठी टिप्स:

1. 📎 ईमेल अटॅचमेंट उघडताना काळजी घ्या
2. 💽 पेन ड्राईव्ह वापरण्याआधी स्कॅन करा
3. 🔗 अनोळखी लिंक्सवर क्लिक करू नका
4. 🚫 पायरटेड सॉफ्टवेअर डाउनलोड करू नका
5. ⚠️ "OK" वर क्लिक करू नका – विशेषतः पॉपअप जाहिराती किंवा खोट्या बक्षिसांवर
6. 🛡️ अँटी-व्हायरस सॉफ्टवेअर इंस्टॉल करा

7. ☁ डेटा क्लाऊड किंवा USB मध्ये बॅकअप ठेवा

🚨 मालवेअर असल्याची लक्षणे:

- 🐢 संगणक संथ होतो
- ❄ वारंवार फ्रीज किंवा क्रॅश होतो
- 📢 विचित्र जाहिराती दिसतात
- 📩 तुमचे अकाउंट आपोआप मेसेज पाठवते
- 📂 अनोळखी ॲप्स आपोआप उघडतात
- 💾 स्टोरेज अचानक भरते

🧹 मालवेअर काढून टाकण्यासाठी काय करावे?

1. 🔌 संगणक इंटरनेटपासून डिस्कनेक्ट करा
2. 🖥 **Safe Mode** मध्ये सुरू करा
3. 🛡 अँटीव्हायरस इंस्टॉल किंवा अपडेट करून स्कॅन करा
4. 🗑 अलीकडे इन्स्टॉल केलेले संशयास्पद ॲप्स काढा
5. 🧽 ब्राउझर कॅशे साफ करा
   Chrome → History → Clear Browsing Data → All Time → Clear
6. 🔁 Safe Mode मधून बाहेर पडण्यासाठी संगणक रिस्टार्ट करा

🆘 समस्या अजूनही सुटली नाही?

तर खालील पर्याय वापरा:
• ऑपरेटिंग सिस्टम पुन्हा इंस्टॉल करा
• तंत्रज्ञान तज्ज्ञाची मदत घ्या

✨ नेहमी लक्षात ठेवा:

• तुमची खासगी माहिती ऑनलाइन शेअर करू नका
• क्लिक करण्यापूर्वी विचार करा
• शंका असल्यास प्रौढ व्यक्तीला विचारा

सुरक्षित राहा. शहाणपणानं वापर करा. 🚀

सायबर दादागिरी
CYBER BULLYING

❌ सायबर बुलींग म्हणजे काय?

सायबर बुलींग म्हणजे एखाद्याला **फोन, संगणक किंवा इंटरनेट** चा वापर करून दुखावणे, चिडवणे, धमकावणे किंवा अपमानित करणे.

हे कुठे होऊ शकते:
• सोशल मीडियावर (Instagram, WhatsApp, Facebook)
• चॅट रूम किंवा मेसेजिंग ॲप्सवर
• ऑनलाइन गेम्समध्ये

🤦‍♀️ प्रत्यक्षातील घटना

इयत्ता ९ वी तील एक हुशार मुलगी अचानक गप्प आणि उदास झाली.
तीचे बोलणे, खाणे, हसणे बंद झाले. शिक्षकांनी तिच्या पालकांशी संपर्क साधला आणि काउन्सेलरकडे नेले.
तपासणीअंती समजले की काही सहकाऱ्यांनी तिच्या वजनावरून सोशल मीडियावर तिची चेष्टा केली.
वेळीच मदत मिळाल्याने ती सावरली आणि शिक्षकांनी इतर विद्यार्थ्यांना सायबर बुलींग किती धोकादायक आहे हे समजावले.

🤍 सायबर बुलींगचे प्रकार

1. **फ्लेमिंग / रोस्टिंग / नावं ठेवणे** – ऑनलाईन वाईट शब्द वापरून दुखावणे
   💼 उदा.: कोणाला अपमानास्पद टोपणनावाने हाक मारणे
2. **आउटिंग** – कोणाची खासगी फोटो किंवा गुपिते परवानगीशिवाय शेअर करणे

3. **ट्रोलिंग** – मुद्दाम राग आणणारे किंवा दुखावणारे मेसेज टाकणे
4. **खोट्या अफवा पसरवणे** – ऑनलाईन खोटी माहिती पसरवणे
5. **अयोग्य फोटो पाठवणे** – परवानगीशिवाय वैयक्तिक फोटो शेअर करणे
6. **सायबर स्टॉकिंग** – वारंवार मेसेज करून घाबरवणे किंवा धमकावणे

🧠 सायबर बुलींगचा बळी झाल्यास परिणाम

- तणाव आणि चिंता
- नैराश्य (खूप उदास वाटणे)
- आत्मविश्वास कमी होणे
- शाळा टाळणे
- लवकर राग येणे किंवा भावनिक होणे

🚨 सायबर बुली कोण असतो?

सायबर बुली असलेली व्यक्ती:
- स्वतःला ताकदवान समजते
- वाईट वागणूक किंवा मानसिक समस्या असू शकतात
- दुसऱ्यांच्या भावना लक्षात घेत नाही

💭 काय करावे आणि काय टाळावे

✅ करावयाच्या गोष्टी:

1. अपमानास्पद मेसेजचा **स्क्रीनशॉट घ्या**

2. **बुलीला ब्लॉक करा**
3. **शिक्षक, पालक किंवा विश्वासू प्रौढाशी बोला**
4. **ॲप किंवा वेबसाईटवर रिपोर्ट करा**
5. **सायबर क्राईम सेलमध्ये तक्रार नोंदवा (गरज असल्यास)**

❌ टाळावयाच्या गोष्टी:

1. बुलीला **उत्तर देऊ नका**
2. **स्वतःला दोष देऊ नका** किंवा **लाज वाटून घेऊ नका**
3. **गप्प राहू नका**

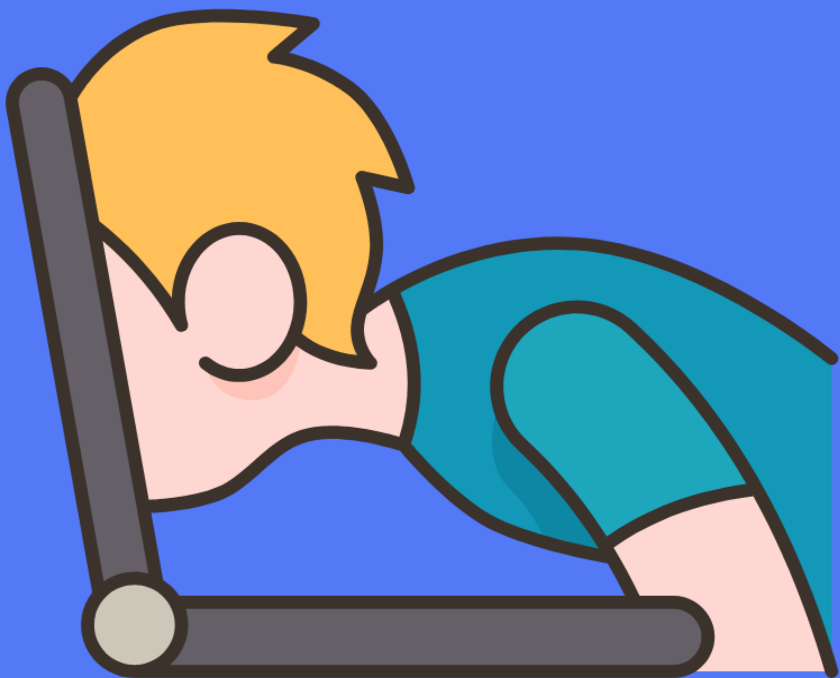
👉 **सायबर बुलींग हा गुन्हा आहे**. कायद्यानुसार त्याला शिक्षा होऊ शकते.

✉️ अंतिम संदेश

बुलींगला नाही म्हणा.
ऑनलाइन दयाळू वागा.
कोणावर तरी अन्याय होताना दिसल्यास आवाज उठवा आणि मदत करा.

What is Bullying?
Cyber bullying is bullying that takes place when someone uses technology to harass, threaten, or target another person.
Impact of Bullying
Fat
Ouning
A-9-tch clas girl student stopped participating, aing and became depressed.
Teachers and parents took action and counseled students on impact of cyber bullying
Precautions to be taken
Don't respond to bellully
Take a screenshot of the post
Block the bully
Talk to a trusted adult
Report to the social media site
REPORT
Reporting
Cybercrime ais a cyber'cime
Cyber bullying is
Say No t Bullying
Cyber Bullying is a cyber crime

गेमिंग आणि सायबर ग्रूमिंग
GAMING & CYBER GROOMING



🎮 ऑनलाइन गेमिंग – मजा पण धोकेही

🚨 ऑनलाइन गेमिंगचे धोके

1. 💻 **हॅकिंग** – वाईट लिंक्स किंवा फाईल्समुळे तुमची वैयक्तिक माहिती चोरी होऊ शकते.
2. 😡 **सायबर बुलींग** – चॅट्स किंवा मेसेजेसच्या माध्यमातून दुसऱ्याला दुखावणे.
3. 🎭 **सायबर ग्रूमिंग** – अनोळखी व्यक्ती मित्र असल्याचा बहाणा करून फसवतात.
4. 💳 **आर्थिक माहिती चोरी**
5. 💰 **सायबर गुन्ह्यांमध्ये वापरणे**

⚠️ धोकादायक टास्क/चॅलेंज गेम्स

काही गेम्समध्ये स्वतःला किंवा इतरांना दुखापत करण्याचे टास्क दिले जातात.
उदाहरणार्थ:
🔷 PUBG
🔷 ब्लू व्हेल
🔷 पिंक सिटी
🔷 पोकेमॉन गो

📍 **खरी घटना:** पिंपरी-चिंचवडमध्ये १४ वर्षांचा मुलगा एका गेम चॅलेंजमुळे बाल्कनीवरून उडी मारून खाली पडला.

🛡️ ऑनलाइन गेमिंगसाठी सुरक्षा टिप्स

1. 🎮 तुमच्या वयानुसार असलेले गेम्सच खेळा.
2. ⏱️ गेम खेळण्याची वेळ मर्यादित ठेवा.
3. 🚫 अनोळखी लोकांबरोबर गेम खेळू नका.
4. 📥🛑 अनोळखी वेबसाईट्सवरून गेम्स डाउनलोड करू नका.
5. 📒📵 तुमची वैयक्तिक माहिती शेअर करू नका.
6. 💳🔒 कार्ड किंवा बँक माहिती गुप्त ठेवा.
7. 🎤📷 व्हॉइस चॅट किंवा वेबकॅम टाळा.
8. 🚷 ऑनलाइन मैत्री करून कधीच एकटे भेटू नका.
9. 🛑📢 काहीतरी अयोग्य वाटल्यास – **ब्लॉक आणि रिपोर्ट करा.**

👀 सायबर ग्रूमिंग म्हणजे काय?

सायबर ग्रूमिंग म्हणजे एखादी व्यक्ती ऑनलाइन मुलांशी विश्वास निर्माण करून त्यांचा **गैरफायदा घेते** किंवा त्यांना **फसवते/धमकावते**.

🧠 सायबर बुलींग आणि ग्रूमिंगपासून वाचण्यासाठी टिप्स

1. तुमची वैयक्तिक माहिती ऑनलाइन शेअर करू नका.
2. फक्त ओळखीच्या लोकांशीच बोला.
3. जर कोणी खूप लवकर मैत्री करू पाहत असेल, तर सावध रहा.
4. जर कोणी फोटो, व्हिडीओ किंवा विचित्र गोष्टी मागत असेल – **ब्लॉक करा.**
5. कधीही ऑनलाइन मित्रांना एकटे भेटू नका.

6. पालक किंवा शिक्षकांशी बोला.
7. **सायबर क्राईम पोलीस** किंवा cybercrime.gov.in वर तक्रार करा.

🌳 मैदानी खेळ का चांगले असतात? 🏃‍♀️🏏

✔ टीमवर्कवाढते
✔ शारीरिक ताकद वाढते
✔ खऱ्या आयुष्यातले मित्र मिळतात

कृत्रिम बुद्धिमत्ता (AI) ची आव्हाने

AI CHALLENGE

AI आणि सायबर सुरक्षा – शहाणे व्हा, सुरक्षित राहा!

📌 AI म्हणजे काय?

AI (आर्टिफिशियल इंटेलिजन्स) म्हणजे अशी तंत्रज्ञान प्रणाली जी संगणकांना माणसांप्रमाणे विचार आणि कृती करायला शिकवते. हे गेम्स, सोशल मीडियामध्ये, ॲप्समध्ये वापरले जाते. पण काही वेळा याचा **गैरवापर** देखील होऊ शकतो. म्हणूनच आपण **सावध राहणे आवश्यक** आहे!

🛑 सायबर जगतात AI चा धोका

1. 📞 **बनावट मेसेज किंवा कॉल्स**
   AI माणसासारखे वाटणारे आवाज तयार करू शकते.
2. 🎥 **डीपफेक व्हिडिओ किंवा फोटो**
   AI बनावट व्हिडिओ किंवा फोटो तयार करून लोकांना फसवते.
3. 💬 **माणसासारखे वाटणारे AI चॅटबॉट्स**
   AI चॅटबॉट्स खऱ्या व्यक्तीसारखे बोलतात आणि तुमची माहिती मिळवण्याचा प्रयत्न करतात.
4. 🧠 **वैयक्तिक माहिती चोरी**
   AI तुमचे ऑनलाइन वर्तन पाहून तुमची माहिती जमा करते.

✅ AI च्या गैरवापरापासून सुरक्षित राहण्यासाठी उपाय

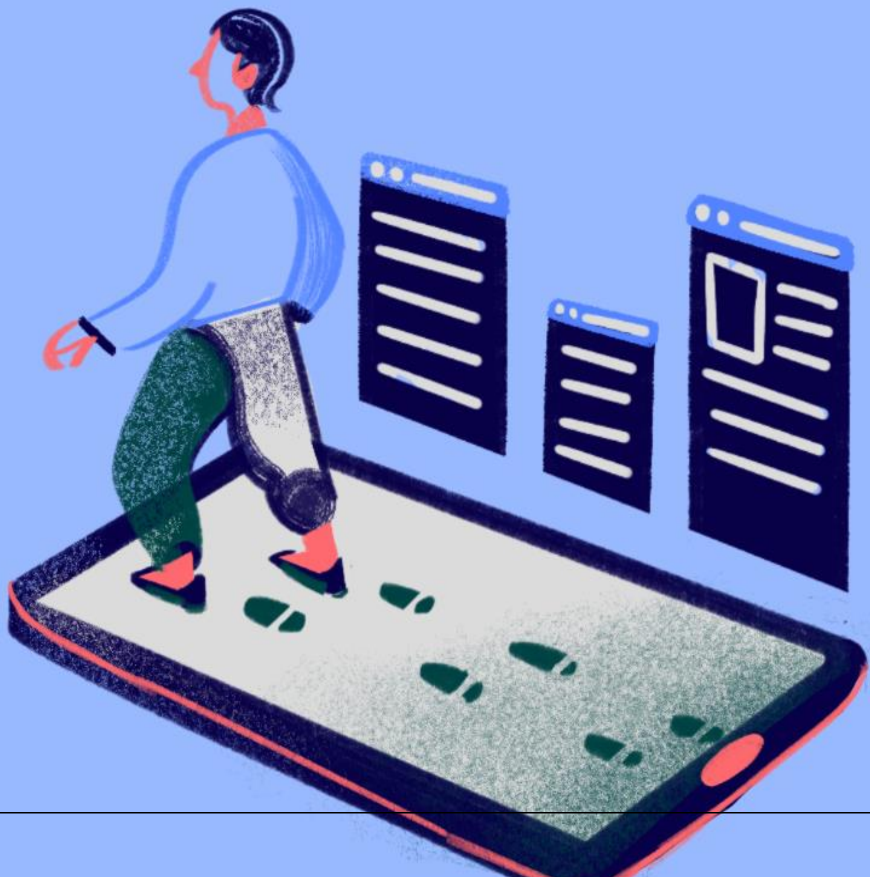
1. 🏫📱 **कधीही तुमचे नाव, शाळेचे नाव, फोन नंबर किंवा पत्ता अनोळखी व्यक्तीला ऑनलाइन देऊ नका.**
2. 🗣️🤖 **माणूस आहे की बॉट हे ओळखा:**
   सोपे प्रश्न विचारा. उत्तरं यंत्रासारखी वाटली तर चॅट थांबवा.
3. 🧠 **विचार करा आणि मगच विश्वास ठेवा:**
   प्रत्येक फोटो, व्हिडिओ किंवा मेसेजवर विश्वास ठेऊ नका – तो AI ने बनवलेला असू शकतो.
4. 🖱️🔗 **अनोळखी लिंक्सवर क्लिक करू नका:**
   AI बॉट्स धोकादायक लिंक्स पाठवू शकतात.
5. 👦💻 **पालकांचे नियंत्रण व सुरक्षा ॲप्स वापरा:**
   वाईट वेबसाईट्स किंवा बॉट्सपासून बचावासाठी पालकांना फिल्टर लावायला सांगा.
6. 🚨 **बनावट किंवा संशयास्पद व्यक्ती दिसल्यास रिपोर्ट करा:**
   कोणी विचित्र वागल्यास शिक्षक किंवा पालकांना सांगा.

🙋 लक्षात ठेवा!

• AI उपयुक्त असू शकते, पण गैरवापर झाल्यास धोकादायक ठरू शकते.
• नेहमी जागरूक राहा आणि सायबर सुरक्षेचे नियम पाळा.

👦✨ शहाणे राहा, सुरक्षित राहा, ऑनलाइन आनंदी राहा!

इंटरनेटचे व्यसन ,सायबर फूटप्रिंट
INTERNET ADDICTION, CYBER FOOTPRINT



🌐 इंटरनेट व्यसन, सेल्फी व्यसन आणि सायबर फूटप्रिंट

📱 इंटरनेट व्यसन म्हणजे काय?

जेव्हा कोणी खूप वेळ ऑनलाइन घालवतो आणि त्याचा परिणाम त्यांच्या:

- आरोग्यावर 🤒
- अभ्यासावर 🎓
- कुटुंब व मित्रांशी संबंधांवर 👨‍👩‍👧
- दैनंदिन जीवनशैलीवर 🕒

होतो, तेव्हा त्याला इंटरनेटचे व्यसन झाल्याचे समजते.

📌 इंटरनेटवर कोणते व्यसन होऊ शकते?

1. वेबसाइट्स सतत पाहणे 🌍
2. गेम खेळत राहणे 🕹️
3. सोशल मीडियाचा अतीव वापर (Instagram, YouTube) 📸
4. अशोभनीय कंटेंट पाहणे 👎

🧠 लोक व्यसनात का अडकतात?

ऑनलाइन गोष्टी मेंदूत **डोपामिन** नावाचे रसायन सोडतात, जे आपल्याला आनंदी वाटण्याची भावना देते. ही भावना पुन्हा-पुन्हा हवीशी वाटते आणि व्यसन निर्माण होते.

✅ इंटरनेट व्यसन कमी करण्याचे उपाय

1. फोन/कॉम्प्युटर वापराची वेळ मर्यादित करा.
2. कला, संगीत, खेळ यासारखी छंद जोपासा.
3. झोपण्याआधी उपकरणे वापरणे टाळा.
4. कुटुंब व चांगल्या मित्रांशी वेळ घालवा.
5. जेवताना मोबाईलचा वापर टाळा.
6. परिस्थिती गंभीर असल्यास समुपदेशकाची मदत घ्या.

🤳 सेल्फी व्यसन म्हणजे काय?

सेल्फी व्यसन म्हणजे सतत सेल्फी घेणे आणि ती सोशल मीडियावर टाकणे – फक्त लाईक्स आणि लक्ष वेधून घेण्यासाठी.

📉 हे कसे अपायकारक ठरू शकते:

- आत्मविश्वास कमी होतो
- स्वतःबद्दल वाईट वाटते
- धोकादायक वागणूक निर्माण होते

📍**खरी घटना:** महाराष्ट्रातील एका सोशल मिडिया इन्फ्लुएन्सरचा सेल्फी घेताना धबधब्याजवळ घसरून मृत्यू झाला.

✅ सेल्फी व्यसन टाळण्यासाठी उपाय

1. सेल्फी घेण्याची व पोस्ट करण्याची मर्यादा ठेवा.
2. क्षणाचा आनंद घ्या, फक्त फोटो घेऊ नका.
3. छंद किंवा खेळांमधून आत्मविश्वास वाढवा.
4. मित्र/कुटुंबाची मदत घ्या.

5. जास्त त्रास होत असेल तर तज्ज्ञांची मदत घ्या.

🧭 सायबर फूटप्रिंट म्हणजे काय?

जसे आपण वाळूत पाऊल टाकल्यावर ठसा राहतो, तसेच **आपण ऑनलाइन जे काही करतो त्याचा डिजिटल ठसा (Cyber Footprint)** राहतो. मात्र असे ठसे नाहीसे होत नाहीत, ते कायमचे राहतात .

📍 यात समाविष्ट आहे:

- आपण भेट दिलेल्या वेबसाइट्स
- आपण शेअर/लाईक केलेल्या पोस्ट्स
- सर्च हिस्टरी
- वैयक्तिक माहिती

🕵️‍♀️ हे कोण पाहू शकतात?

- महाविद्यालये
- नोकरी देणाऱ्या कंपन्या
- व्हिसा अधिकारी
- भविष्यकालीन विवाह भागीदार देखील!

✅ आपली डिजिटल छाप स्वच्छ ठेवण्यासाठी उपाय

1. काय पोस्ट करता हे विचारपूर्वक करा.
2. वैयक्तिक माहिती ऑनलाइन देऊ नका.
3. अशाश्वत किंवा अशोभनीय वेबसाइट्स टाळा.
4. कॉमेंट्स किंवा मेसेज पाठवताना आधी विचार करा.

5. स्वतःचे नाव गुगल करून तपासा – दुसऱ्यांना काय दिसते?

💡 **शेवटचा सल्ला:**

इंटरनेट वापरा – पण शहाणपणाने
ते एक साधन आहे, तुमचा मालक नाही!

मूलभूत ऑनलाईन आर्थिक सुरीक्षितता
BASIC ONLINE FINANCIAL SAFETY

💰 ऑनलाइन पैश्याचे व्यवहार करताना सायबर सुरक्षा

🏬 आर्थिक व्यवहार म्हणजे काय?

आर्थिक व्यवहार म्हणजे ऑनलाइन पैसे पाठवणे किंवा मिळवणे, जसे की:

- UPI वापरणे (Google Pay, PhonePe वगैरे)
- ऑनलाइन खरेदी करणे
- डेबिट/क्रेडिट कार्ड वापरणे
- शाळेच्या फीचा ऑनलाइन भरणा

🚨 काळजी का घ्यावी लागते?

जर आपण काळजी घेतली नाही, तर **हॅकर्स व फसवणूक करणारे**:

- तुमचे पैसे चोरू शकतात 💸
- तुमची वैयक्तिक माहिती मिळवू शकतात 📄
- तुमचे खाते गैरवापरासाठी वापरू शकतात ⚠️

✅ पैशांचे व्यवहार करताना सायबर सुरक्षा नियम

1. 🔒 **फक्त सुरक्षित व खात्रीशीर ॲप्स वापरा**
   ✅ Google Pay, PhonePe, Paytm किंवा तुमच्या बँकेचे

अधिकृत ॲप वापरा.
❌ अनोळखी किंवा बनावट ॲप्स वापरू नका.

---

2. 🤐 **OTP किंवा PIN कधीच शेअर करू नका**
खालील गोष्टी कोणालाही सांगू नका – अगदी मित्रांनाही नाही:

- ATM PIN
- UPI PIN
- OTP (One-Time Password)

---

3. 📧 **अनोळखी लिंक्सवर क्लिक करू नका**
फसवणूक करणारे बनावट लिंक्स, मेसेज किंवा ईमेलद्वारे पाठवतात.
❌ त्यावर क्लिक करू नका.
✅ अधिकृत वेबसाइट्स वापरा.

---

4. 💳 **पब्लिक डिव्हाइसेसवर कार्ड डिटेल्स सेव्ह करू नका**
खालील ठिकाणी कार्ड डिटेल्स सेव्ह करणे टाळा:

- सायबर कॅफे
- मित्राचा फोन
- सार्वजनिक कॉम्प्युटर

---

5. 👀 **पैसे पाठवण्याआधी तपासणी करा**
✅ नाव व नंबर नीट तपासा.

❌ लहान चूक झाल्यास पैसे चुकीच्या व्यक्तीकडे जाऊ शकतात.

---

6. 👦🏫 **पालक किंवा शिक्षकांना सांगा**
   जर काहीतरी चुकीचे वाटले किंवा घडले तर:

- ताबडतोब पालक किंवा शिक्षकांना सांगा.
- आर्थिक चुका लपवू नका.

---

7. 🚨 **फसवणूक झाल्यास त्वरित रिपोर्ट करा**
   जर पैसे चोरीला गेले, तर:

- तुमच्या बँकेच्या ग्राहक सेवा क्रमांकावर त्वरित फोन करा.
- cybercrime.gov.in वर रिपोर्ट करा.

🌟 चतुर विद्यार्थी = सुरक्षित विद्यार्थी!

ऑनलाइन पैसे वापरणे फायदेशीर आहे – पण **फक्त तेव्हा जेव्हा तुम्ही शहाणपणे, सुरक्षितपणे आणि सतर्क राहता.**

तक्रार नोंदवण्याचेमाध्यम
REPORTING CHANNELS

🚨 सायबर गुन्हे रिपोर्ट कसे करावेत

सायबर गुन्ह्यांमध्ये दिवसेंदिवस वाढ होत आहे. भारतात आणि इतर देशांतील **हॅकर्स आणि फसवणूक करणारे,** लोकांना फसवण्यासाठी हुशारीने ट्रिक्स वापरतात.
🧠 म्हणूनच सायबर गुन्हे **वेळेत रिपोर्ट करणे खूप महत्त्वाचे आहे.**

❓ सायबर गुन्हे का रिपोर्ट करावेत?

1. ✅ तुमची समस्या लवकर सुटू शकते.
2. 🛑 इतरांना फसवणुकीपासून वाचवता येते.
3. 💸 **1 तासाच्या आत आर्थिक फसवणूक रिपोर्ट केली, तर 90% पैसे परत मिळू शकतात.**
4. 👮 पोलिस कारवाई करू शकतात आणि इतरांचे संरक्षण करता येते.

📍 सायबर गुन्हे कुठे आणि कसे रिपोर्ट करायचे 👇?

1. 🏢 ऑफलाइन: जवळच्या सायबर क्राइम पोलिस स्टेशनमध्ये जा

पुणे पोलिस सायबर सेल

📧 ईमेल: crimecyber.pune@nic.in
📞 फोन: 020-29710097

---

2. 🌐 ऑनलाइन: सरकारचा सायबर क्राइम पोर्टलचा वापरा

🔗 वेबसाईट: https://cybercrime.gov.in
🛡️ हे सर्व सायबर गुन्ह्यांचे रिपोर्टिंगसाठी अधिकृत व सुरक्षित पोर्टल आहे.
🚺 **स्त्री व बालकांविरुद्ध गुन्हे नाव न देता** देखील येथे रिपोर्ट करता येतात.

---

3. ☎️ सायबर क्राइम हेल्पलाईन क्रमांक

- 📞 **1930** – राष्ट्रीय सायबर गुन्हे हेल्पलाईन
    - 📞**1945-** महाराष्ट्र सायबर गुन्हे हेल्पलाईन

- 👶 **1098** – चाइल्डलाइन इंडिया (बालकांविरुद्ध गुन्ह्यांसाठी)

---

4. 📱 सोशल मीडियावर रिपोर्ट करा

Cyber Dost – गृह मंत्रालयाने सुरू केलेला अधिकृत सायबर सुरक्षा अकाऊंट

- 🐦 X (Twitter): **@CyberDost**
- 📘 Facebook: **Cyber Dost**
- 📷 Instagram: **Cyber Dost**
- 📲 Telegram: **Cyber Dost Channel**

---

5. 📡 टेलिकॉम विभागात रिपोर्ट करा

🔗 वेबसाईट: https://sancharsaathi.gov.in
फोनशी संबंधित फसवणुकीसाठी हे पोर्टल उपयुक्त आहे.

🛠️ **Sanchar Saathi वर उपलब्ध सेवा:**
• 🔎 **CHAKSHU** – फेक मेसेज/कॉल तपासणी
• 📵 **CEIR** – हरवलेला किंवा चोरीचा फोन ब्लॉक करा
• 📱 **TAFCOP** – तुमच्या नावावर किती नंबर आहेत ते पहा
• 🔢 **KYM** – मोबाईलचा IMEI नंबर तपासा
• ☎️ **RICWIN** – भारतीय नंबरवरून आलेले फेक कॉल्स रिपोर्ट करा
• 🌐 **ISP तपासणी** – इंटरनेट सेवा प्रदात्याची माहिती मिळवा
📞 हेल्पलाईन: **14022**

🧠 लक्षात ठेवा:

🚦 **ऑनलाइन सतर्क रहा.**
👦🏫 शंका आल्यास विश्वासू शिक्षक किंवा पालकांना त्वरित सांगा.
🔐 **तुमचे वेळीच उचलेले पाऊल सायबर गुन्हा थांबवू शकते आणि कुणाचे तरी पैसे किंवा जीव वाचवू शकते!**

आभार प्रदर्शन

• "Be Cyber Safe" कार्यक्रमासाठी पूर्ण सहकार्य केल्याबद्दल आम्ही पुणे पोलिसांचे मन: पूर्वक आभार मानतो.
• या पुस्तकातील मजकूर पडताळून सत्यापित केल्याबद्दल सायबर कायदा तज्ज्ञ ॲड. वैशाली भागवत यांचे मन: पूर्वक आभार.
• मौल्यवान सूचना दिल्याबद्दल सायबर सुरक्षा समन्वयक, संगणकशास्त्र विभाग, फर्ग्युसन कॉलेज, पुणे येथील सहाय्यक प्राध्यापक डॉ. आरती समीर निमगावकर यांचे मनःपूर्वक आभार.

रोटरी क्लब ऑफ पूना वेस्ट टीम

• अध्यक्ष: रोटे. संतोष चिपळूणकर
• सेवा संचालक: रोटे. भाग्यश्री भिडे
• सायबर सुरक्षा समिती अध्यक्षा: रोटे. रीता कोठारी
• संकल्पना, मजकूर निर्मिती, व्हिडीओ सादरीकरण: रोटे. डॉ. माधुरी घाटे
• मजकूर संपादन व मराठी भाषांतर: रोटे. भाग्यश्री भिडे

धन्यवाद!

तुम्ही सायबर सुरक्षित राहायला शिकलात!