ZARURAT APP Present with

Cyber World Awareness Quiz Competion

Exam Syllabus

आवश्यक दिशा निर्देश -

1- अध्ययन के लये सलेबस में 300 प्रश्न है जिनमें से 50 MCQ (बहु वकल्पी प्रश्नपूछे (जायेंगे सलेबस ! ! डाउनलोड कर लें

2- सभी प्रतिभागी ' डजिटल सहभ गता प्रमाण पत्र' https://udaanonline.in/ से डाउनलोड कर सकते है!

3- टेस्ट की तारीख आपके वद्यालय के द्वारा बताई जायेगी, ऑनलाइन टेस्ट रात 8.30 बजे से होगा !

4- क्लास -4th से लेकर 8th तक के बच्चों को 50 मनट में उत्तर देना है जब क क्लास -9th के ऊपर के बच्चों को 30 मनट में उत्तर देना है!

Chapter – 1) परिचय

1. **सवाल:** साइबर क्राइम से आप क्या समझते हैं?
   उत्तर: इंटरनेट, कंप्यूटर या डिजिटल नेटवर्क के माध्यम से किया गया अपराध साइबर क्राइम कहलाता है।
2. **सवाल:** साइबर अपराध और पारंपरिक अपराध में क्या अंतर है?
   उत्तर: पारंपरिक अपराध भौतिक रूप से होता है जबकि साइबर अपराध डिजिटल माध्यम से किया जाता है।
3. **सवाल:** आईटी एक्ट 2000 कब लागू हुआ?
   उत्तर: भारत में आईटी एक्ट 2000, **17 अक्टूबर 2000** को लागू हुआ।
4. **सवाल:** साइबर कानून क्यों आवश्यक है?
   उत्तर: साइबर अपराधों को रोकने, नियंत्रण करने और दोषियों को दंडित करने के लिए।
5. **सवाल:** साइबर अपराध के मुख्य कारण क्या हैं?
   उत्तर: लालच, जानकारी की कमी, तकनीकी दुरुपयोग, कमजोर सुरक्षा व्यवस्था।
6. **सवाल:** भारत में पहला साइबर अपराध कब दर्ज हुआ?
   उत्तर: 2001 में इंटरनेट पर "याहू चैट रूम" से जुड़ा केस।
7. **सवाल:** "हैकिंग" किस प्रकार का अपराध है?
   उत्तर: कंप्यूटर/नेटवर्क में बिना अनुमति प्रवेश करना।
8. **सवाल:** साइबर अपराध के कितने प्रकार होते हैं?
   उत्तर: मुख्य रूप से 5 – हैकिंग, वित्तीय धोखाधड़ी, साइबर बुलिंग, पोर्नोग्राफी, डेटा चोरी।
9. **सवाल:** साइबर अपराध का समाज पर क्या प्रभाव पड़ता है?
   उत्तर: आर्थिक नुकसान, मानसिक तनाव, गोपनीयता भंग होना।
10. **सवाल:** साइबर अपराध रोकने के लिए क्या उपाय हैं?
    उत्तर: मजबूत पासवर्ड, टू-फैक्टर ऑथेंटिकेशन, एंटीवायरस, सुरक्षित नेटवर्क।

Chapter – 2) साइबर क्राइम के प्रकार

11. **सवाल:** फ़िशिंग (Phishing) किसे कहते हैं?
    उत्तर: नकली ईमेल/वेबसाइट के जरिए यूज़र से जानकारी चुराना।
12. **सवाल:** विशिंग (Vishing) क्या है?
    उत्तर: फोन कॉल के जरिए धोखा देकर जानकारी लेना।
13. **सवाल:** स्मिशिंग (Smishing) क्या है?
    उत्तर: SMS के जरिए फ्रॉड करना।
14. **सवाल:** मालवेयर (Malware) क्या है?
    उत्तर: ऐसा हानिकारक सॉफ़्टवेयर जो सिस्टम को नुकसान पहुंचाए।
15. **सवाल:** वायरस और वर्म में अंतर बताइए।
    उत्तर: वायरस को फैलने के लिए होस्ट फाइल चाहिए, वर्म खुद-ब-खुद फैलता है।
16. **सवाल:** रैनसमवेयर (Ransomware) क्या है?
    उत्तर: ऐसा मालवेयर जो डेटा को लॉक कर पैसे मांगता है।
17. **सवाल:** ट्रोजन हॉर्स क्या है?
    उत्तर: उपयोगी दिखने वाला लेकिन अंदर से हानिकारक सॉफ़्टवेयर।
18. **सवाल:** कीलॉगर (Keylogger) क्या करता है?
    उत्तर: यूज़र द्वारा दबाई गई कुंजियों को रिकॉर्ड करता है।
19. **सवाल:** स्पाइवेयर (Spyware) क्या है?
    उत्तर: गुप्त रूप से यूज़र की गतिविधि पर नजर रखने वाला सॉफ़्टवेयर।
20. **सवाल:** बॉटनेट (Botnet) किसे कहते हैं?
    उत्तर: हैकर द्वारा नियंत्रित संक्रमित कंप्यूटरों का नेटवर्क।
21. **सवाल:** DoS अटैक क्या है?
    उत्तर: किसी सर्वर/वेबसाइट को ट्रैफिक से भरकर बंद करना।
22. **सवाल:** DDoS और DoS अटैक में अंतर क्या है?
    उत्तर: DoS में एक सिस्टम से हमला, DDoS में कई सिस्टम से।
23. **सवाल:** वेब जैकिंग क्या है?
    उत्तर: वेबसाइट का नियंत्रण छीन लेना।
24. **सवाल:** साइबर स्क्वॉटिंग क्या है?
    उत्तर: प्रसिद्ध ब्रांड नाम के समान डोमेन खरीदकर बेचना।
25. **सवाल:** ई-मेल स्पूफिंग क्या है?
    उत्तर: नकली ईमेल भेजकर धोखा देना।
26. **सवाल:** साइबर पोर्नोग्राफी क्या है?
    उत्तर: इंटरनेट पर अश्लील सामग्री का प्रसार।
27. **सवाल:** साइबर बुलिंग किसे कहते हैं?
    उत्तर: ऑनलाइन गाली, धमकी या परेशान करना।

28. **सवाल:** साइबर स्टॉकिंग क्या है?
उत्तर: किसी को लगातार ऑनलाइन परेशान/फॉलो करना।
29. **सवाल:** आइडेंटिटी थेफ्ट (Identity Theft) क्या है?
उत्तर: किसी की निजी जानकारी चुराकर अपराध करना।
30. **सवाल:** क्रेडिट कार्ड फ्रॉड किस श्रेणी में आता है?
उत्तर: वित्तीय साइबर अपराध।

Chapter – 3) : सोशल मीडिया और अपराध

31. **सवाल:** फेक आईडी क्या है?
उत्तर: किसी दूसरे नाम से बनाई गई नकली प्रोफाइल।
32. **सवाल:** सोशल मीडिया पर साइबर बुलिंग कैसे होती है?
उत्तर: कमेंट, मैसेज, मीम के जरिए अपमानित करना।
33. **सवाल:** ट्रोलिंग क्या है?
उत्तर: जानबूझकर भड़काऊ/नकारात्मक टिप्पणी करना।
34. **उत्तर:** तस्वीर में बदलाव कर फेक इमेज बनाना।
35. **सवाल:** डीपफेक वीडियो क्या है?
उत्तर: AI तकनीक से नकली वीडियो बनाना।
36. **सवाल:** बच्चों को सोशल मीडिया पर सबसे बड़ा खतरा क्या है?
उत्तर: साइबर बुलिंग और ऑनलाइन शोषण।
37. **सवाल:** साइबर एथिक्स क्यों जरूरी हैं?
उत्तर: सुरक्षित और जिम्मेदार ऑनलाइन व्यवहार के लिए।
38. **सवाल:** ऑनलाइन गेमिंग से जुड़े अपराध कौन से हैं?
उत्तर: पहचान चोरी, धोखाधड़ी, साइबर बुलिंग।
39. **सवाल:** सोशल मीडिया साइबर अपराध में क्या भूमिका निभाता है?
उत्तर: अपराधियों के लिए लोगों तक पहुँचने का आसान माध्यम।
40. सोशल मीडिया पर बच्चों को अश्लील कंटेंट से कैसे बचाया जा सकता है? **उत्तर:** प्राइवेसी सेटिंग्स और अभिभावक की निगरानी
41. बच्चों की ऑनलाइन गतिविधि पर नजर रखने वाला एक ऐप कौनसा है-? **उत्तर :**Google Family Link
42. बच्चों को इंटरनेट पर सुरक्षित व्यवहार सिखाने के लिए क्या जरूरी है? **उत्तर:** साइबर एथिक्स की शिक्षा
43. बच्चों के लिए उपयुक्त सोशल मीडिया ऐप कौनसे हैं-?
उत्तर : YouTube Kids और Messenger Kids
44. बच्चों को ऑनलाइन अश्लीलता की रिपोर्ट करना कैसे सिखाया जा सकता है? **उत्तर :**"Report" और "Block" विकल्प का उपयोग सिखाकर
45. साइबर बुलिंग से बच्चों को बचाने के लिए क्या करना चाहिए? **उत्तर:** डिजिटल सीमाएं सिखाना और खुलकर बात करने के लिए प्रेरित करना
46. फेक आईडी बनाने पर कौन-सी साइबर कानून की धारा लागू होती है? **उत्तर:** आईटी एक्ट की धारा 66C और 66D
47. फेक आईडी से किसी की छवि खराब करना किस कानून के अंतर्गत आता है? **उत्तर:** आईटी एक्ट की धारा 66E और IPC की धारा 500
48. फेक आईडी की शिकायत कहाँ की जा सकती है?
उत्तर: www.cybercrime.gov.in या साइबर सेल में
49. फेक आईडी से पैसे मांगना किस श्रेणी का अपराध है?
उत्तर: साइबर धोखाधड़ी
50. फेक आईडी से जुड़े अपराधों की सजा क्या हो सकती है?
उत्तर: 3 से 7 साल तक की जेल और जुर्माना

Chapter– 3) साइबर सुरक्षा उपाय

51. **सवाल:** मजबूत पासवर्ड क्यों जरूरी है?
उत्तर: ताकि हैकर्स आसानी से अकाउंट हैक न कर सकें।
52. **सवाल:** टू-फैक्टर ऑथेंटिकेशन क्या है?
उत्तर: पासवर्ड के साथ अतिरिक्त सत्यापन (OTP, बायोमेट्रिक आदि)।
53. **सवाल:** फ़ायरवॉल का मुख्य कार्य क्या है?
उत्तर: नेटवर्क को अनधिकृत एक्सेस से बचाना।
54. **सवाल:** एंटीवायरस का उपयोग क्यों किया जाता है?
उत्तर: वायरस और मालवेयर को हटाने के लिए।
55. **सवाल:** डेटा एन्क्रिप्शन का अर्थ क्या है?
उत्तर: डेटा को कोड में बदलकर सुरक्षित करना।
56. **सवाल:** सुरक्षित ब्राउज़िंग के लिए क्या करना चाहिए?
उत्तर: HTTPS वेबसाइट का उपयोग, VPN, ब्राउज़र अपडेट।
57. **सवाल:** साइबर सुरक्षा नीति (Cyber Security Policy) क्या है?
उत्तर: संगठन/देश द्वारा साइबर सुरक्षा के लिए बनाए गए नियम।
58. **सवाल:** बच्चों को साइबर सुरक्षा कैसे सिखाई जा सकती है?
उत्तर: ऑनलाइन खतरे समझाना, स्क्रीन टाइम नियंत्रित करना।
59. **सवाल:** साइबर हाइजीन क्या है?
उत्तर: सुरक्षित डिजिटल आदतें (पासवर्ड बदलना, सॉफ़्टवेयर अपडेट)।
60. **सवाल:** भारत में "राष्ट्रीय साइबर सुरक्षा दिवस" कब मनाया जाता है?
उत्तर: 2 दिसंबर।

Chapter – 4) साइबर कानून

61. **सवाल:** आईटी एक्ट 2000 का उद्देश्य क्या है?
उत्तर: इलेक्ट्रॉनिक लेन-देन को कानूनी मान्यता और साइबर अपराध नियंत्रण।
62. **सवाल:** आईटी एक्ट में कितने अध्याय हैं?
उत्तर: 13 अध्याय।
63. **सवाल:** साइबर अपराध से जुड़ी धारा 66C किससे संबंधित है?
उत्तर: पहचान चोरी (Identity Theft)।
64. **सवाल:** धारा 66D क्या कहती है?
उत्तर: कंप्यूटर माध्यम से धोखाधड़ी।
65. **सवाल:** धारा 67B किस अपराध से संबंधित है?
उत्तर: बच्चों की अश्लील सामग्री।
66. **सवाल:** भारत में साइबर अपराध रिपोर्ट कहाँ की जा सकती है?
उत्तर: cybercrime.gov.in पोर्टल पर।
67. **सवाल:** साइबर अपील अधिकरण (Cyber Appellate Tribunal) क्यों बनाया गया?
उत्तर: आईटी एक्ट से जुड़े मामलों की सुनवाई के लिए।
68. **सवाल:** आईटी एक्ट 2008 में क्या संशोधन हुआ?
उत्तर: साइबर आतंकवाद और डेटा सुरक्षा को शामिल किया गया।
69. **सवाल:** साइबर अपराध से जुड़ी भारतीय दंड संहिता (IPC) की धारा कौन सी है?
उत्तर: धारा 463-465 (जालसाजी), 499 (मानहानि), 420 (धोखाधड़ी)।
70. **सवाल:** साइबर कानून क्यों जरूरी है?
उत्तर: ताकि डिजिटल अपराधों पर कानूनी कार्रवाई हो सके।

Chapter- 5) : साइबर अपराध और समाज

71. **सवाल:** साइबर अपराध से युवाओं पर क्या प्रभाव पड़ता है?
उत्तर: पढ़ाई पर असर, मानसिक तनाव, आर्थिक नुकसान।
72. **सवाल:** साइबर अपराध का शिक्षा क्षेत्र पर क्या असर है?
उत्तर: ऑनलाइन कक्षाओं में हैकिंग/अनुचित सामग्री का खतरा।
73. **सवाल:** साइबर अपराध का व्यापार पर क्या प्रभाव है?
उत्तर: डेटा चोरी, वित्तीय हानि, प्रतिष्ठा का नुकसान।
74. **सवाल:** ऑनलाइन गेमिंग से किस प्रकार के अपराध बढ़ते हैं?
उत्तर: साइबर बुलिंग, पहचान चोरी, वित्तीय धोखाधड़ी।
75. **सवाल:** साइबर अपराध का महिलाओं पर क्या असर है?
उत्तर: ऑनलाइन उत्पीड़न, मॉर्फिंग, स्टॉकिंग।
76. **सवाल:** साइबर अपराध का बच्चों पर क्या प्रभाव है?
उत्तर: गलत सामग्री, ऑनलाइन शोषण, मानसिक स्वास्थ्य पर असर।
77. **सवाल:** साइबर अपराध का देश की सुरक्षा पर क्या असर है?
उत्तर: साइबर आतंकवाद, सैन्य डेटा लीक।
78. **सवाल:** साइबर अपराध और गोपनीयता (Privacy) में क्या संबंध है?
उत्तर: अपराध अक्सर निजी जानकारी चुराकर होता है।
79. **सवाल:** साइबर अपराध का पत्रकारिता पर क्या असर है?
उत्तर: फेक न्यूज और गलत सूचना का प्रसार।
80. **सवाल:** समाज को साइबर अपराध से बचाने का सबसे बड़ा तरीका क्या है?
उत्तर: साइबर जागरूकता।

Chapter – 6) तकनीकी शब्दावली

81. **सवाल:** स्पैम मेल क्या है?
उत्तर: अवांछित और अनचाहे ईमेल।
82. **सवाल:** ईव्सड्रॉपिंग (Eavesdropping) क्या है?
उत्तर: बिना अनुमति बातचीत/डेटा सुनना।
83. **सवाल:** स्निफिंग (Sniffing) किसे कहते हैं?
उत्तर: नेटवर्क से डेटा पैकेट चोरी करना।
84. **सवाल:** स्पूफिंग (Spoofing) क्या है?
उत्तर: नकली पहचान से हमला करना।
85. **सवाल:** SQL Injection क्या है?
उत्तर: डेटाबेस में अनधिकृत कोड डालकर डेटा चोरी करना।
86. **सवाल:** ब्रूट फोर्स अटैक क्या है?
उत्तर: बार-बार पासवर्ड ट्रायल करके हैक करना।
87. **सवाल:** ज़ॉम्बी कंप्यूटर (Zombie Computer) क्या है?
उत्तर: हैकर के नियंत्रण में आया संक्रमित कंप्यूटर।
88. **सवाल:** पेलोड (Payload) क्या होता है?
उत्तर: मालवेयर का वह हिस्सा जो असली नुकसान करता है।
89. **सवाल:** बैकडोर (Backdoor) क्या है?
उत्तर: सिस्टम में गुप्त प्रवेश मार्ग।
90. **सवाल:** क्लिकजैकिंग (Clickjacking) क्या है?
उत्तर: यूज़र को नकली बटन क्लिक कराने की तकनीक।

Chapter – 7) साइबर अपराध रोकथाम

91. **सवाल:** साइबर अपराध रोकने का पहला कदम क्या है?
उत्तर: यूज़र की जागरूकता।
92. **सवाल:** साइबर सुरक्षा में "अपडेट" क्यों जरूरी है?
उत्तर: नई कमजोरियों से बचाने के लिए।
93. **सवाल:** साइबर हेल्पलाइन नंबर क्या है?
उत्तर: 1930 (भारत में)।
94. **सवाल:** साइबर पुलिस की भूमिका क्या है?
उत्तर: साइबर अपराध की जांच और गिरफ्तारी।
95. **सवाल:** CERT-In क्या है?
उत्तर: भारत की कंप्यूटर इमरजेंसी रिस्पॉन्स टीम।

96. **सवाल:** बग बाउंटी प्रोग्राम क्या है?
उत्तर: सॉफ़्टवेयर की खामियां खोजने पर इनाम देना।
97. **सवाल:** डिजिटल साक्षरता क्यों जरूरी है?
उत्तर: ताकि लोग साइबर अपराध से बच सकें।
98. **सवाल:** VPN का उपयोग क्यों किया जाता है?
उत्तर: सुरक्षित और प्राइवेट इंटरनेट ब्राउज़िंग के लिए।
99. **सवाल:** CAPTCHA का उपयोग क्यों होता है?
उत्तर: बॉट्स को रोकने और मानव उपयोगकर्ता की पहचान के लिए।
100. **सवाल:** साइबर अपराध से बचने का सबसे सरल उपाय क्या है?
उत्तर: संदिग्ध लिंक/ईमेल पर क्लिक न करना।

Chapter – 8) : साइबर अपराध के उदाहरण

101. **सवाल:** सबसे आम साइबर अपराध कौन सा है?
उत्तर: फ़िशिंग (Phishing)।
102. **सवाल:** साइबर आतंकवाद (Cyber Terrorism) क्या है?
उत्तर: राष्ट्र की सुरक्षा, सैन्य या महत्वपूर्ण ढांचे को नुकसान पहुँचाने के लिए इंटरनेट का उपयोग।
103. **सवाल:** साइबर अपराध में "डार्क वेब" क्या भूमिका निभाता है?
उत्तर: डार्क वेब पर अवैध सामान, हथियार, डेटा और ड्रग्स बेचे जाते हैं।
104. **सवाल:** ऑनलाइन लॉटरी फ्रॉड किस प्रकार का अपराध है?
उत्तर: वित्तीय धोखाधड़ी।
105. **सवाल:** साइबर अपराध में फेक न्यूज का क्या महत्व है?
उत्तर: अफवाहें फैलाना और समाज में अशांति पैदा करना।
106. **सवाल:** रैनसमवेयर अटैक से बचने का उपाय क्या है?
उत्तर: डेटा का बैकअप और एंटी-मालवेयर का प्रयोग।
107. **सवाल:** सोशल मीडिया हैकिंग का मतलब क्या है?
उत्तर: बिना अनुमति किसी की प्रोफ़ाइल/अकाउंट को एक्सेस करना।
108. **सवाल:** ई-मेल हैकिंग क्यों की जाती है?
उत्तर: पासवर्ड रीसेट करना, गोपनीय डेटा चुराना।
109. **सवाल:** साइबर अपराध में "डेटा ब्रीच" क्या है?
उत्तर: बड़ी मात्रा में डेटा का लीक होना।
110. **सवाल:** पायरेसी (Piracy) किसे कहते हैं?
उत्तर: बिना अनुमति फिल्म, सॉफ़्टवेयर या संगीत की कॉपी और वितरण।

Chapter – 9) : राष्ट्रीय और अंतर्राष्ट्रीय स्तर

111. **सवाल:** भारत में साइबर अपराध की जांच कौन करता है?
उत्तर: साइबर पुलिस और CBI।
112. **सवाल:** इंटरपोल साइबर क्राइम यूनिट का क्या कार्य है?
उत्तर: अंतर्राष्ट्रीय साइबर अपराध से निपटना।
113. **सवाल:** CERT-In की स्थापना कब हुई?
उत्तर: 2004 में।
114. **सवाल:** NCIIPC का फुल फॉर्म क्या है?
उत्तर: National Critical Information Infrastructure Protection Centre।
115. **सवाल:** साइबर अपराध पर अंतर्राष्ट्रीय समझौता कौन सा है?
उत्तर: बुडापेस्ट कन्वेंशन।
116. **सवाल:** भारत में "डिजिटल इंडिया" अभियान कब शुरू हुआ?
उत्तर: 1 जुलाई 2015।
117. **सवाल:** साइबर क्राइम को रोकने के लिए सरकार कौन सा पोर्टल चलाती है?
उत्तर: cybercrime.gov.in

118. **सवाल:** साइबर अपराध में "Interpol 24x7" क्या है?
उत्तर: त्वरित सूचना साझा करने का नेटवर्क।
119. **सवाल:** ITU किस क्षेत्र से संबंधित है?
उत्तर: अंतर्राष्ट्रीय दूरसंचार और साइबर सुरक्षा।
120. **सवाल:** Europol किस प्रकार काम करता है?
उत्तर: यूरोप में साइबर अपराध रोकने के लिए।

Chapter -9) : साइबर अपराध और तकनीकी खतरे

121. **सवाल:** IoT डिवाइस साइबर अपराध के लिए क्यों संवेदनशील हैं?
उत्तर: इनकी सुरक्षा कमजोर होती है।
122. **सवाल:** स्मार्टफोन हैकिंग कैसे होती है?
उत्तर: मालवेयर, फेक ऐप, असुरक्षित वाई-फाई से।
123. **सवाल:** पब्लिक वाई-फाई का खतरा क्या है?
उत्तर: हैकर्स डेटा इंटरसेप्ट कर सकते हैं।
124. **सवाल:** क्लाउड सुरक्षा क्यों जरूरी है?
उत्तर: क्योंकि डेटा क्लाउड सर्वर पर स्टोर होता है।
125. **सवाल:** डीप वेब और डार्क वेब में क्या अंतर है?
उत्तर: डीप वेब सुरक्षित निजी डेटा होता है, डार्क वेब अवैध गतिविधियों के लिए।
126. **सवाल:** स्मार्ट होम डिवाइस में कौन सा अपराध संभव है?
उत्तर: डेटा चोरी और जासूसी।
127. **सवाल:** बायोमेट्रिक डेटा चोरी किस अपराध में आता है?
उत्तर: आइडेंटिटी थेफ्ट।
128. **सवाल:** मोबाइल ट्रोजन क्या है?
उत्तर: मोबाइल में हानिकारक ऐप जो डेटा चोरी करता है।
129. **सवाल:** क्रिप्टोजैकिंग (Cryptojacking) क्या है?
उत्तर: किसी के कंप्यूटर का उपयोग गुप्त रूप से क्रिप्टो माइनिंग के लिए करना।
130. **सवाल:** साइबर अपराध में ड्रोन का उपयोग कैसे हो सकता है?
उत्तर: अवैध निगरानी और डेटा चोरी के लिए।

Chapter – 10) साइबर अपराध और शिक्षा

131. **सवाल:** ई-लर्निंग प्लेटफ़ॉर्म पर किस प्रकार के साइबर अपराध हो सकते हैं?
उत्तर: डेटा चोरी, ज़ूम बॉम्बिंग, फेक लिंक।
132. **सवाल:** ऑनलाइन परीक्षा में सबसे आम अपराध क्या है?
उत्तर: हैकिंग और चीटिंग।
133. **सवाल:** ऑनलाइन क्लास में "Zoom Bombing" क्या है?
उत्तर: क्लास में अनधिकृत व्यक्ति घुसना और अशोभनीय गतिविधि करना।
134. **सवाल:** छात्र साइबर अपराध से कैसे बच सकते हैं?
उत्तर: पासवर्ड साझा न करें, सुरक्षित लिंक उपयोग करें।
135. **सवाल:** साइबर जागरूकता अभियान का उद्देश्य क्या है?
उत्तर: लोगों को डिजिटल सुरक्षा के प्रति सचेत करना।
136. **सवाल:** डिजिटल साक्षरता मिशन कब शुरू हुआ?
उत्तर: 2014 में (PMGDISHA योजना के तहत)।
137. **सवाल:** बच्चे किस प्रकार साइबर अपराध का शिकार होते हैं?
उत्तर: साइबर बुलिंग, गेमिंग फ्रॉड, अश्लील सामग्री।
138. **सवाल:** "साइबर एथिक्स" स्कूल में क्यों पढ़ाया जाता है?
उत्तर: बच्चों में जिम्मेदार डिजिटल व्यवहार विकसित करने के लिए।
139. **सवाल:** कॉलेज छात्रों पर साइबर अपराध का क्या असर है?
उत्तर: मानसिक तनाव और पढ़ाई में बाधा।
140. **सवाल:** शिक्षा संस्थानों को साइबर सुरक्षा के लिए क्या करना चाहिए?
उत्तर: सुरक्षित नेटवर्क, साइबर अवेयरनेस वर्कशॉप।

Chapter – 11) : केस स्टडी और उदाहरण

141. **सवाल:** WannaCry हमला किस प्रकार का साइबर अटैक था?
उत्तर: रैनसमवेयर अटैक।
142. **सवाल:** पेट्या/NotPetya अटैक किस वर्ष हुआ?
उत्तर: 2017।
143. **सवाल:** भारत में "Cosmos Bank" हैकिंग किस वर्ष हुई?
उत्तर: 2018।
144. **सवाल:** आधार डेटा ब्रीच किस प्रकार का अपराध था?
उत्तर: व्यक्तिगत डेटा चोरी।
145. **सवाल:** कैम्ब्रिज एनालिटिका केस किससे संबंधित है?
उत्तर: फेसबुक यूज़र्स का डेटा चोरी।
146. **सवाल:** साइबर आतंकवाद का उदाहरण दीजिए।
उत्तर: पाकिस्तान द्वारा भारतीय वेबसाइट हैक करना।
147. **सवाल:** साइबर अपराध में "Morris Worm" क्यों प्रसिद्ध है?
उत्तर: पहला कंप्यूटर वर्म (1988)।
148. **सवाल:** माइक्रोसॉफ्ट एक्सचेंज सर्वर हैकिंग कब हुई?
उत्तर: 2021।
149. **सवाल:** भारतीय रेल टिकटिंग वेबसाइट IRCTC पर किस प्रकार का अटैक हुआ था?
उत्तर: डेटा चोरी।
150. **सवाल:** सबसे बड़ा ईमेल हैकिंग केस कौन सा है?
उत्तर: Yahoo डेटा ब्रीच (2013-2014)।

Chapter -12) : आधुनिक साइबर अपराध

151. **सवाल:** स्पीयर फ़िशिंग (Spear Phishing) क्या है?
उत्तर: किसी खास व्यक्ति/संगठन को टारगेट करके किया गया फ़िशिंग हमला।
152. **सवाल:** व्हेलिंग (Whaling) अटैक क्या है?
उत्तर: कंपनी के बड़े अधिकारियों को टारगेट कर धोखाधड़ी करना।
153. **सवाल:** साइबर जासूसी (Cyber Espionage) क्या है?
उत्तर: गोपनीय सरकारी/सैन्य जानकारी चोरी करना।
154. **सवाल:** ईमेल बमबारी (Email Bombing) क्या है?
उत्तर: किसी व्यक्ति को हजारों ईमेल भेजकर सिस्टम क्रैश करना।
155. **सवाल:** क्रॉस-साइट स्क्रिप्टिंग (XSS) क्या है?
उत्तर: वेबसाइट में कोड डालकर यूज़र डेटा चोरी करना।
156. **सवाल:** वाई-फाई हैकिंग किस प्रकार का अपराध है?
उत्तर: अनधिकृत रूप से नेटवर्क का उपयोग करना।
157. **सवाल:** साइबर ब्लैकमेलिंग क्या है?
उत्तर: निजी फोटो/वीडियो से धमकी देकर पैसा वसूलना।
158. **सवाल:** कार्डिंग (Carding) क्या है?
उत्तर: चोरी किए गए क्रेडिट/डेबिट कार्ड से खरीदारी करना।
159. **सवाल:** बिटकॉइन स्कैम क्या है?
उत्तर: नकली क्रिप्टोकरेंसी स्कीम से लोगों को ठगना।
160. **सवाल:** सॉफ्टवेयर पायरेसी क्यों अपराध है?
उत्तर: यह कॉपीराइट उल्लंघन है।

Chapter -13) :: साइबर अपराध में कानून और सज़ा

161. **सवाल:** धारा 65 आईटी एक्ट किससे संबंधित है?
उत्तर: कंप्यूटर स्रोत दस्तावेज़ से छेड़छाड़।
162. **सवाल:** धारा 66F किस अपराध से संबंधित है?
उत्तर: साइबर आतंकवाद।
163. **सवाल:** धारा 67 क्या कहती है?
उत्तर: अश्लील सामग्री का प्रकाशन/प्रसारण अपराध है।
164. **सवाल:** पहचान चोरी (Identity Theft) पर क्या सज़ा है?
उत्तर: 3 साल की कैद और ₹1 लाख जुर्माना।
165. **सवाल:** साइबर आतंकवाद पर अधिकतम सज़ा क्या है?
उत्तर: आजीवन कारावास।
166. **सवाल:** एटीएम/कार्ड फ्रॉड किस धारा के अंतर्गत आता है?
उत्तर: धारा 66C और 66D।
167. **सवाल:** साइबर अपराध की रिपोर्ट कितने घंटे में करनी चाहिए?
उत्तर: 24 घंटे के भीतर।

168. **सवाल:** नाबालिग द्वारा साइबर अपराध करने पर क्या होता है?
उत्तर: किशोर न्याय अधिनियम के तहत कार्रवाई।
169. **सवाल:** IPC धारा 420 किस अपराध से संबंधित है?
उत्तर: धोखाधड़ी।
170. **सवाल:** साइबर क्राइम पर त्वरित न्याय के लिए क्या व्यवस्था है?
उत्तर: साइबर अपीलीय अधिकरण।

Chapter -14) : साइबर अपराध और सुरक्षा एजेंसियाँ

171. **सवाल:** NCIIPC का मुख्य कार्य क्या है?
उत्तर: महत्वपूर्ण सूचना अवसंरचना की सुरक्षा।
172. **सवाल:** IB और RAW किस प्रकार साइबर अपराध में सहयोग करते हैं?
उत्तर: राष्ट्रीय सुरक्षा और जासूसी मामलों में।
173. **सवाल:** DRDO साइबर सुरक्षा में क्या भूमिका निभाता है?
उत्तर: सैन्य नेटवर्क और सिस्टम की सुरक्षा।
174. **सवाल:** गृह मंत्रालय का "I4C" क्या है?
उत्तर: Indian Cyber Crime Coordination Centre।
175. **सवाल:** इंटरपोल का साइबर क्राइम केंद्र कहाँ है?
उत्तर: सिंगापुर।
176. **सवाल:** Europol का मुख्यालय कहाँ है?
उत्तर: द हेग, नीदरलैंड्स।
177. **सवाल:** FBI की साइबर डिवीजन क्या करती है?
उत्तर: अमेरिका में साइबर अपराध की जांच।
178. **सवाल:** साइबर अपराध में "Blue Whale Game" क्यों बदनाम हुआ?
उत्तर: यह ऑनलाइन गेम बच्चों को आत्महत्या के लिए उकसाता था।
179. **सवाल:** साइबर सुरक्षा हेल्पलाइन 1930 किस मंत्रालय के अधीन है?
उत्तर: गृह मंत्रालय।
180. **सवाल:** साइबर स्वच्छता केंद्र का उद्देश्य क्या है?
उत्तर: नागरिकों को मुफ्त सुरक्षा उपकरण उपलब्ध कराना।

Chapter -15) : जागरूकता और रोकथाम

181. **सवाल:** "Think Before You Click" का क्या मतलब है?
उत्तर: किसी भी लिंक/ईमेल पर क्लिक करने से पहले जांचें।
182. **सवाल:** साइबर अपराध से बचने के लिए छात्रों को क्या करना चाहिए?
उत्तर: पासवर्ड साझा न करें, सुरक्षित ऐप का उपयोग करें।
183. **सवाल:** साइबर सुरक्षा में पेरेंटल कंट्रोल क्यों जरूरी है?
उत्तर: बच्चों को हानिकारक कंटेंट से बचाने के लिए।
184. **सवाल:** फेक न्यूज़ से कैसे बचा जा सकता है?
उत्तर: स्रोत की पुष्टि करें और सत्यापन करें।
185. **सवाल:** साइबर जागरूकता अभियान क्यों जरूरी है?
उत्तर: लोगों को सुरक्षित डिजिटल व्यवहार सिखाने के लिए।
186. **सवाल:** ऑफिस में साइबर सुरक्षा के लिए क्या उपाय हैं?
उत्तर: VPN, एंटीवायरस, फायरवॉल, स्टाफ ट्रेनिंग।
187. **सवाल:** पब्लिक कंप्यूटर पर लॉगिन करने के बाद क्या करना चाहिए?
उत्तर: Logout करना और Cache साफ करना।
188. **सवाल:** सोशल मीडिया पर निजी जानकारी साझा करने से क्या खतरे हैं?
उत्तर: पहचान चोरी और ब्लैकमेलिंग।
189. **सवाल:** ईमेल पासवर्ड कितने समय में बदलना चाहिए?
उत्तर: हर 3-6 महीने में।
190. **सवाल:** OTP को गोपनीय क्यों रखना चाहिए?
उत्तर: क्योंकि यह लेन-देन का सुरक्षा कोड होता है।

Chapter -16) : भविष्य और साइबर अपराध

191. **सवाल:** AI का दुरुपयोग साइबर अपराध में कैसे हो सकता है?
उत्तर: डीपफेक, ऑटोमेटेड हैकिंग, फेक न्यूज़।
192. **सवाल:** 5G तकनीक से साइबर अपराध का खतरा क्यों बढ़ेगा?
उत्तर: तेज़ स्पीड और अधिक डिवाइस कनेक्शन।
193. **सवाल:** क्वांटम कंप्यूटिंग साइबर सुरक्षा के लिए खतरा क्यों है?
उत्तर: यह मौजूदा एन्क्रिप्शन तोड़ सकता है।
194. **सवाल:** ब्लॉकचेन साइबर सुरक्षा में कैसे मदद करता है?
उत्तर: डेटा को सुरक्षित और अपरिवर्तनीय बनाता है।
195. **सवाल:** भविष्य में साइबर युद्ध (Cyber War) क्या हो सकता है?
उत्तर: देशों के बीच डिजिटल हमले।
196. **सवाल:** बायोमेट्रिक हैकिंग क्या है?
उत्तर: फिंगरप्रिंट/आईरिस स्कैन जैसी पहचान चुराना।
197. **सवाल:** क्लाउड हैकिंग क्या है?
उत्तर: क्लाउड सर्वर पर स्टोर डेटा चोरी करना।
198. **सवाल:** वॉइस फिशिंग (Voice Phishing) का भविष्य में उपयोग कैसे होगा?
उत्तर: AI से नकली आवाज बनाकर धोखा देना।
199. **सवाल:** साइबर अपराध से लड़ने के लिए सबसे बड़ी चुनौती क्या है?
उत्तर: तकनीक का तेज़ विकास और सीमाओं से परे अपराध।
200. **सवाल:** साइबर अपराध को रोकने का सबसे प्रभावी तरीका क्या है?
उत्तर: साइबर जागरूकता, मजबूत कानून और उन्नत तकनीक।

Chapter -12) : बैंक संबंधित धोखाधड़ी !

201. **बैंक फ्रॉड क्या है?**
उत्तर: धोखे से बैंक या ग्राहक से पैसा हड़पना।

202. **सबसे कॉमन बैंक फ्रॉड कौन सा है?**
उत्तर: ATM कार्ड और ऑनलाइन ट्रांजैक्शन फ्रॉड।

203. **फ्रॉड में OTP का इस्तेमाल कैसे होता है?**
उत्तर: OTP लेकर अकाउंट से पैसा निकाला जाता है।

204. **फिशिंग क्या है?**
उत्तर: नकली ईमेल/वेबसाइट से जानकारी चोरी करना।

205. **स्मिशिंग क्या है?**
उत्तर: SMS से धोखाधड़ी करना।

206. **विशिंग क्या है?**
उत्तर: फोन कॉल से धोखाधड़ी करना।

207. **कार्ड क्लोनिंग क्या है?**
उत्तर: कार्ड की कॉपी बनाकर इस्तेमाल करना।

208. **ATM स्किमिंग क्या है?**
उत्तर: ATM मशीन पर डिवाइस लगाकर डेटा चोरी करना।

209. **बैंक KYC कॉल पर जानकारी मांगता है?**
उत्तर: नहीं।

210. **QR कोड स्कैन करने से हमेशा पैसा मिलता है?**
उत्तर: नहीं, पैसा कट सकता है।

Chapter -13) : ATM और कार्ड फ्रॉड

211. **ATM PIN किसे बताना चाहिए?**
उत्तर: किसी को भी नहीं।

212. **अगर ATM कार्ड मशीन में फंस जाए तो?**
उत्तर: तुरंत बैंक हेल्पलाइन को कॉल करें।

213. **ATM से पैसा निकलते समय क्या सावधानी रखें?**
उत्तर: PIN छुपाकर डालें।

214. **CVV नंबर कहाँ होता है?**
उत्तर: कार्ड के पीछे 3 अंकों का कोड।

215. **ATM रिसीट किसे देनी चाहिए?**
उत्तर: किसी को नहीं।

216. **डुप्लीकेट कार्ड कैसे बनता है?**
उत्तर: क्लोनिंग/स्किमिंग से।

217. **ATM पर भीड़ होने पर क्या करें?**
उत्तर: सुरक्षित ATM पर जाएँ।

218. **ATM पिन कितनी बार बदलना चाहिए?**
उत्तर: समय-समय पर।

219. **ATM फ्रॉड रोकने का मुख्य तरीका?**
उत्तर: सुरक्षित मशीन का उपयोग।

220. **कार्ड शेयर करना सुरक्षित है?**
उत्तर: नहीं।

Chapter -14) ऑनलाइन बैंकिंग

221. **नेटबैंकिंग पासवर्ड कितनी बार बदलना चाहिए?**
उत्तर: हर 3–6 महीने में।

222. **ऑनलाइन ट्रांजैक्शन के लिए किस लिंक का इस्तेमाल करें?**
उत्तर: https से शुरू होने वाले।

223. **बैंक OTP मांगता है?**
उत्तर: कभी नहीं।

224. **फर्जी ईमेल कैसे पहचानें?**
उत्तर: उसमें गलत लिंक और इनाम का झांसा होता है।

225. **पब्लिक Wi-Fi पर नेटबैंकिंग करना चाहिए?**
उत्तर: नहीं।

226. **नेटबैंकिंग के लिए कौन सा ब्राउज़र सुरक्षित है?**
उत्तर: अपडेटेड ब्राउज़र।

227. **पासवर्ड में क्या होना चाहिए?**
उत्तर: अक्षर, अंक और स्पेशल कैरेक्टर।

228. **पासवर्ड किसी को बताना चाहिए?**
उत्तर: नहीं।

229. **नेटबैंकिंग लॉगिन कहाँ से करें?**
उत्तर: बैंक की आधिकारिक वेबसाइट से।

230. **फिशिंग ईमेल का पहला लक्षण क्या है?**
उत्तर: अजीब लिंक और डराने वाली भाषा।

Chapter -15) UPI और मोबाइल फ्रॉड

231. **UPI PIN कितने अंकों का होता है?**
उत्तर: 4 या 6।

232. **UPI पिन किसे बताना चाहिए?**
उत्तर: किसी को भी नहीं।

233. **UPI में पैसा कैसे कटता है?**
उत्तर: रिक्वेस्ट मंजूर करने पर।

234. **QR कोड से पैसा कैसे चोरी होता है?**
उत्तर: स्कैन करने पर अकाउंट से पैसा निकल सकता है।

235. **Paytm/PhonePe ऐप कहाँ से डाउनलोड करें?**
उत्तर: प्ले स्टोर या ऐप स्टोर से।

236. **मोबाइल पर स्क्रीन शेयरिंग ऐप क्यों खतरनाक है?**
उत्तर: फ्रॉडस्टर सब देख सकता है।

237. **अनजान लिंक से ऐप डाउनलोड करना सुरक्षित है?**
उत्तर: नहीं।

238. **मोबाइल नंबर अपडेट क्यों जरूरी है?**
उत्तर: SMS अलर्ट पाने के लिए।

239. **UPI में ऑटो-डिडक्शन को कैसे रोका जाए?**
उत्तर: ऑटोमैंडेट कैंसल करें।

240. **UPI ऐप लॉक क्यों जरूरी है?**
उत्तर: अतिरिक्त सुरक्षा के लिए।

Chapter -16) कॉल और SMS फ्रॉड

241. **KYC कॉल असली होती है?**
उत्तर: नहीं।

242. **इनाम जीतने का SMS असली होता है?**
उत्तर: नहीं।

243. **फ्रॉड कॉल पर क्या करें?**
उत्तर: कॉल काटें और ब्लॉक करें।

244. **बैंक कर्मचारी फोन पर पासवर्ड मांगता है?**
उत्तर: नहीं।

245. **अज्ञात लिंक पर क्लिक करना चाहिए?**
उत्तर: नहीं।

246. **SMS में अकाउंट ब्लॉक लिखकर लिंक दिया हो तो?**
उत्तर: क्लिक न करें।

247. **कस्टमर केयर नंबर कहाँ से लें?**
उत्तर: बैंक की वेबसाइट से।

248. **WhatsApp पर बैंक लिंक असली होता है?**
उत्तर: नहीं।

249. **RBI ग्राहकों को कॉल करता है?**
उत्तर: नहीं।

250. **SMS अलर्ट क्यों जरूरी है?**
उत्तर: हर ट्रांजैक्शन की जानकारी के लिए।

Chapter -17) लोन और इन्वेस्टमेंट फ्रॉड

251. **लोन फ्रॉड क्या है?**
उत्तर: नकली एजेंट पैसे लेकर भाग जाना।

252. **लॉटरी मेल असली होता है?**
उत्तर: नहीं।

253. **जॉब ऑफर के नाम पर पैसे मांगना क्या है?**
उत्तर: रोजगार फ्रॉड।

254. **इन्वेस्टमेंट स्कैम की पहचान कैसे करें?**
उत्तर: बहुत ज्यादा रिटर्न का झांसा।

255. **लोन प्रोसेसिंग फीस कहाँ देनी चाहिए?**
उत्तर: केवल बैंक अकाउंट में।

256. **इनाम जीतने पर फीस भरनी चाहिए?**
उत्तर: नहीं।

257. **फर्जी लोन ऐप कहां से आते हैं?**
उत्तर: थर्ड पार्टी वेबसाइट से।

258. **बैंक कभी लोन के लिए घर पर कैश लेता है?**
उत्तर: नहीं।

259. **लोन स्कैम से बचने का तरीका?**
उत्तर: सिर्फ आधिकारिक बैंक से आवेदन करना।

260. **नकली इन्वेस्टमेंट कंपनी कैसे पहचानें?**
उत्तर: उसका कोई रजिस्टर्ड लाइसेंस नहीं होता।

Chapter -18) टेक्निकल सुरक्षा

261. **2FA का मतलब क्या है?**
उत्तर: टू फैक्टर ऑथेंटिकेशन।

262. **एन्क्रिप्शन क्यों जरूरी है?**
उत्तर: डेटा को सुरक्षित रखने के लिए।

263. **स्किमिंग डिवाइस कहाँ लगाई जाती है?**
उत्तर: ATM मशीन पर।

264. **सिक्योरिटी पिन का उपयोग कहाँ होता है?**
उत्तर: ATM और UPI में।

265. **मजबूत पासवर्ड क्यों जरूरी है?**
उत्तर: अकाउंट सुरक्षा के लिए।

266. **वन-टाइम पासवर्ड (OTP) कितनी देर तक मान्य होता है?**
उत्तर: कुछ मिनट।

267. **फायरवॉल किसलिए होता है?**
उत्तर: नेटवर्क को सुरक्षित रखने के लिए।

268. **एंटीवायरस ऐप क्यों जरूरी है?**
उत्तर: मोबाइल/कंप्यूटर को सुरक्षित रखने के लिए।

269. **स्मार्टफोन में स्क्रीन लॉक क्यों जरूरी है?**
उत्तर: अकाउंट डेटा सुरक्षित रखने के लिए।

270. **SIM स्वैपिंग क्या है?**
उत्तर: नया SIM बनवाकर अकाउंट कंट्रोल लेना।

Chapter -19) रिपोर्टिंग और लॉ

271. **फ्रॉड होने पर पहला कदम क्या है?**
उत्तर: बैंक को सूचित करना।

272. **फ्रॉड की शिकायत कहाँ करें?**
उत्तर: साइबर सेल में।

273. **साइबर क्राइम हेल्पलाइन नंबर क्या है?**
उत्तर: 1930।

274. **साइबर क्राइम रिपोर्टिंग वेबसाइट कौन सी है?**
उत्तर: cybercrime.gov.in।

275. **क्या FIR दर्ज कराना जरूरी है?**
उत्तर: हाँ।

276. **फ्रॉड रिपोर्ट कब करनी चाहिए?**
उत्तर: तुरंत।

277. **क्या बैंक ग्राहक की मदद करता है फ्रॉड में?**
उत्तर: हाँ।

278. **क्या ग्राहक का पैसा वापस मिल सकता है?**
उत्तर: समय पर रिपोर्ट करने पर हाँ।

279. **क्या पुलिस बैंक फ्रॉड केस लेती है?**
उत्तर: हाँ।

280. **फ्रॉड रिपोर्ट करने से क्या फायदा होता है?**
उत्तर: जांच और पैसे वापस मिलने की संभावना।

Chapter -20) केस स्टडी टाइप

281. **₹10 भेजकर फ्रॉड कैसे होता है?**
उत्तर: टेस्ट करके बाद में बड़ी रकम निकाल लेते हैं।

282. **"आपका अकाउंट ब्लॉक हो जाएगा" वाला SMS क्या है?**
उत्तर: फिशिंग मैसेज।

283. **"आपने लॉटरी जीती" वाला ईमेल क्या है?**
उत्तर: स्कैम।

284. **जॉब ऑफर देकर पैसे मांगना क्या है?**
उत्तर: फ्रॉड।

285. **विदेश से इनाम आने का मेल असली होता है?**
उत्तर: नहीं।

286. **WhatsApp पर KYC अपडेट लिंक कैसा होता है?**
उत्तर: नकली।

287. **UPI पर पैसे लेने के लिए पिन डालना पड़ता है?**
उत्तर: नहीं, सिर्फ भेजने के लिए।

288. **कोई कहे "Google Form भरो और ₹500 मिलेगा", तो क्या है?**
उत्तर: फ्रॉड।

289. **कस्टमर केयर स्कैम कैसे होता है?**
उत्तर: नकली नंबर देकर।

290. **मोबाइल ऐप इंस्टॉल करवाकर डेटा चोरी करना क्या है?**
उत्तर: ऐप फ्रॉड।

Chapter -21) सुरक्षा टिप्स

291. **बैंक पासबुक की कॉपी किसे देनी चाहिए?**
उत्तर: किसी को नहीं।

292. **सुरक्षित लेन-देन के लिए क्या जरूरी है?**
उत्तर: OTP और पासवर्ड गोपनीय रखना।

293. **SMS अलर्ट क्यों जरूरी है?**
उत्तर: हर ट्रांजैक्शन की जानकारी मिलती है।

294. **ईमेल में अटैचमेंट खोलते समय क्या ध्यान दें?**
उत्तर: केवल भरोसेमंद भेजने वाले का खोलें।

295. **ATM पर कोई मदद करने आए तो?**
उत्तर: इंकार करें।

296. **फ्रॉड रोकने के लिए मोबाइल अपडेट क्यों जरूरी है?**
उत्तर: सिक्योरिटी पैच मिलता है।

297. **क्या पब्लिक कंप्यूटर पर नेटबैंकिंग करनी चाहिए?**
उत्तर: नहीं।

298. **क्या बैंक कभी फोन पर पासवर्ड मांगेगा?**
उत्तर: कभी नहीं।

299. **कस्टमर को खुद से क्या जांचना चाहिए?**
उत्तर: बैंक स्टेटमेंट।

300. **बैंक फ्रॉड से बचने का सबसे अच्छा तरीका?**
उत्तर: सतर्क रहना और जानकारी सुरक्षित रखना।

Attention please

भारत में साइबर क्राइम से जुड़ी शकायत दर्ज कराने के लए सरकार ने कुछ आ धकारिक प्लेटफ़ॉर्म और हेल्पलाइन नंबर जारी कए हैं। आप इनका इस्तेमाल कर सकते हैं!

1. ऑनलाइन शकायत प्लेटफ़ॉर्म

- राष्ट्रीय साइबर क्राइम रिपोर्टिंग पोर्टल
  https://cybercrime.gov.in
  इस पोर्टल पर आप ऑनलाइन धोखाधड़ी, सोशल मी डया पर उत्पीड़न, साइबर बु लंग, ऑनलाइन वत्तीय फ्रॉड, आदि की शकायत दर्ज कर सकते हैं।

2. हेल्पलाइन नंबर

- साइबर क्राइम हेल्पलाइन नंबर : **1930**
  (पहले यह 155260 था, अब इसे बदलकर 1930 कर दिया गया है(
  इस नंबर पर कॉल करके आप तुरंत शकायत दर्ज करा सकते हैं, खासकर अगर ऑनलाइन धोखाधड़ी या पैसों की ठगी हुई हो।

3. पु लस स्टेशन

- आप सीधे अपने नज़दीकी पु लस स्टेशन में जाकर भी साइबर क्राइम की रिपोर्ट लखवा सकते हैं।
- अगर आपके शहर में साइबर क्राइम पु लस स्टेशन है, तो वहाँ जाना सबसे बेहतर रहेगा।

This paper has been composed by
"Advocate Gaurav Tripathi 'Amar'"