माध्यमिक शिक्षा विभाग, उत्तर प्रदेश

साइबर सुरक्षित बेटी

सतर्क,सजग,समझदार

डिजिटल युग में सुरक्षित बेटी

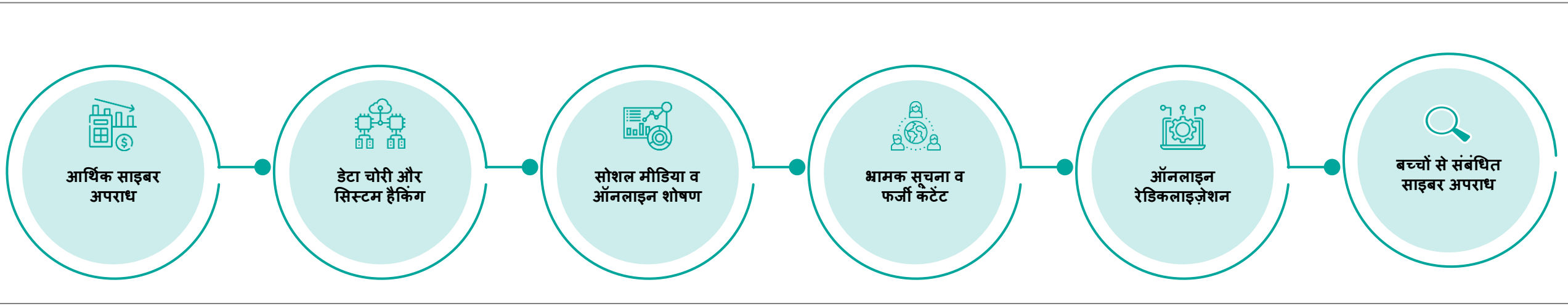
आत्मविश्वास से मुस्कुराती हमारी साइबर सुरक्षित बेटी है,
पढाई,मनोरंजन,सोशल मीडिया का जो लाभ खूब उठाती है|
पर ऑनलाइन अपराधों के खतरों से सतर्क हमेशा रहती है,
अपना हर कदम सावधानी और समझदारी से यह उठाती है|

आओ हम सब साइबर सुरक्षित बेटी बनें |

साइबर अपराध क्या है?

- साइबर क्राइम अपराधों का नया रूप है। यह एक प्रकार की गैर-कानूनी गतिविधि है, जिसे कंप्यूटर, मोबाइल या इंटरनेट के माध्यम से सम्पादित किया जाता है और जिस का मुख्य उद्देश्य किसी की जानकारी, जमा पूंजी और पहचान चुराना है।
- आज साइबर अपराधों ने बहुत तेजी से समाज को जकड़ रखा है। विशेष रूप से लड़कियों के लिए यह ख़तरा और भी विकराल रूप ले चुका है।
- साइबर क्राइम का शिकार बनने के मुख्य कारण किसी पर भी आसानी से भरोसा करना, भयभीत होना और साइबर क्राइम के प्रति अनभिज्ञता है|
- अब समय आ गया है कि सतर्कता, सावधानी और समझदारी से हम सब जागरूक बने और अपनी पहचान, गोपनीयता एवं मर्यादा के प्रति सजग रहें।

साइबर अपराध के प्रकार



उपरोक्त 6 प्रकार के अपराधों को आगे की स्लाइड्स में विस्तार से समझाया गया है। साथ ही उनके लिए क्या करें (Do's) और क्या न करें (Don'ts) भी बताए गए हैं।

1a. आर्थिक साइबर अपराध (Financial Cyber Crimes)

- **Debit Card Cloning**: कार्ड डेटा चोरी कर नकली कार्ड से पैसे निकालना।
- **QR Code Scam**: धोखे से फर्जी QR कोड स्कैन करवा कर पैसे या बैंक जानकारी चुराना।
- **Ponzi Scheme**: जल्दी अमीर बनने का लालच देकर निवेश राशि की ठगी करना।
- **Scratch Card Scam**: इनाम का झांसा देकर लिंक से डेटा चोरी करना।
- **Crypto Fraud**: फर्जी क्रिप्टो साइट बनाकर निवेशकों से पैसा ठगना।
- **Micro Loan Scam:** नकली ऐप से लोन के नाम पर डेटा और पैसा चोरी करना।
- **Session Hijacking**: यूज़र का लॉगिन सेशन चुराकर अकाउंट पर कब्जा करना।
- **Virtual Kidnapping**: झूठा अपहरण दिखाकर फिरौती माँगना।
- **Formjacking**: वेबसाइट फॉर्म में कोड डालकर कार्ड डिटेल चोरी करना।
- **Jumped Deposit**: फर्जी जमा या ट्रांज़ैक्शन से धोखा करना।
- **Cyber Squatting**: ब्रांड नाम से मिलते जुलते डोमेन खरीदकर महंगे दाम पर बेचना।
- **Crypto-jacking:** दूसरों के कंप्यूटर से अवैध रूप से क्रिप्टो माइनिंग करना।

1b. आर्थिक सुरक्षा (Financial Safety)

✅ Do's:

- केवल अधिकृत बैंक और ऐप से ही लेन-देन करें।
- UPI, बैंक या कार्ड लेन-देन की सूचना आने पर तुरंत जांच करें।
- बैंक की आधिकारिक वेबसाइट/ऐप से ही लॉगिन करें।
- किसी भी संदिग्ध कॉल या ईमेल पर तुरंत बैंक हेल्पलाइन से संपर्क करें।
- QR कोड केवल भुगतान करने के लिए ही स्कैन करें।

❌ Don'ts:

- "आपका खाता बंद हो गया" जैसे ईमेल/कॉल पर भरोसा न करें।
- किसी भी तरह के अजनबियों को निजी वित्तीय जानकारी न दें।
- जल्दी अमीर बनने या इनाम जीतने वाले संदेशों पर विश्वास न करें।
- सोशल मीडिया पर अपने बैंक कार्ड की फोटो या जानकारी शेयर न करें।
- सार्वजनिक वाई-फाई से बैंकिंग ऐप न खोलें।

2a. डेटा चोरी और सिस्टम हैकिंग (Data Theft & Hacking Crimes)

- **Keylogger**: टाइपिंग रिकॉर्ड कर पासवर्ड/OTP चोरी — एंटीवायरस लगाएँ।
- **Wi-Fi Hacking**: कमजोर नेटवर्क से डेटा चोरी — मजबूत पासवर्ड रखें।
- **RFID Cloning**: कार्ड सिग्नल कॉपी कर नकली कार्ड बनाना — कार्ड शील्ड उपयोग करें।
- **Profile Hacking**: सोशल मीडिया/मेल हैक करना — मजबूत पासवर्ड व 2FA अपनाएँ।
- **SIM Swap**: फर्जी SIM से OTP लेकर ठगी — SIM बंद होते ही शिकायत करें।
- **Juice Jacking**: पब्लिक चार्जिंग से डेटा चोरी — अपना चार्जर इस्तेमाल करें।
- **Ransomware**: डेटा लॉक कर फिरौती माँगना — बैकअप रखें।
- **App Trap**: फर्जी ऐप से डेटा/पैसे चोरी — केवल आधिकारिक स्टोर से ऐप लें।
- **Steganography**: फोटो/ऑडियो में डेटा छिपाना — संदिग्ध फाइल न खोलें।
- **Prompt Engineering**: रणनीतिक इनपुट से गलत जवाब निकलवाना — सावधानी रखें।
- **Fileless Attack:** बिना फाइल छोड़े सिस्टम पर हमला — एंडपॉइंट सुरक्षा बढ़ाएँ।
- **Insider Threat**: कर्मचारी द्वारा डेटा चोरी — एक्सेस नियंत्रण रखें।
- **LLM Jailbreak**: एआई सुरक्षा तोड़ने की कोशिश — सुरक्षा नीति लागू रखें।

2b. डेटा चोरी और सिस्टम हैकिंग सुरक्षा (Data Theft & Hacking Safety)

✅ Do’s:

- केवल विश्वसनीय ऐप स्टोर से ही ऐप डाउनलोड करें।
- ऐप्स इंस्टॉल करने से पहले समीक्षाएं और अनुमतियां पढ़ें।
- गोपनीयता नीतियों और शर्तों की जाँच करें।
- केवल दो-कारक प्रमाणीकरण वाले ऐप्स का उपयोग करें।
- धोखाधड़ी का प्रयास करने वालों के सबूत (स्क्रीनशॉट, चैट) रखें।

❌ Don’ts:

- ऐप मे संपर्कों या फ़ोटो तक पहुंच जैसी अनावश्यक अनुमति न दें।
- ऐसे ऐप्स से बचें जो बिना किसी सत्यापन के तुरंत ऋण देने का वादा करते हैं।
- अज्ञात नंबरों से प्राप्त लिंक पर क्लिक न करें।
- ऋण एजेंटों को कभी भी अग्रिम धनराशि न दें।
- अनावश्यक बैंक अकाउंटों को न खोलें।

3a. सोशल मीडिया व ऑनलाइन शोषण (Social Exploitation & Cyber Abuse)

- **Cyber Stalking**: किसी व्यक्ति द्वारा बार-बार ऑनलाइन पीछा करना या डराना — यह मानसिक उत्पीड़न है, तुरंत रिपोर्ट करें।
- **Cyber Bullying**: किसी की निजी फोटो या जानकारी सार्वजनिक कर बदनाम करना — यह गंभीर अपराध है, तुरंत रिपोर्ट करें।
- **Fake Profile / Sextortion**: फर्जी प्रोफाइल बनाकर निजी फोटो से ब्लैकमेल करना — अपनी तस्वीरें सीमित लोगों तक रखें।
- **Honey Trap**: नकली रिश्ते बनाकर भावनात्मक ठगी करना — अजनबियों पर भरोसा न करें।
- **Picture Morphing:** किसी की तस्वीर को बदलकर अशोभनीय बनाना — इससे सामाजिक बदनामी होती है।
- **Cyber Grooming**: बच्चों से झूठी पहचान बनाकर गलत उद्देश्य से बातचीत करना — अभिभावक बच्चों पर निगरानी रखें।
- **Deepfake**: कृत्रिम बुद्धिमत्ता (AI) से किसी की आवाज़ या चेहरा बदलकर नकली वीडियो या ऑडियो बनाना।
- **Doxing**: किसी व्यक्ति की निजी जानकारी (जैसे पता, फोन नंबर, फोटो) बिना अनुमति ऑनलाइन सार्वजनिक करना।
- **Social Trolling**: सोशल मीडिया पर अपमानजनक या भड़काऊ टिप्पणियाँ करना — यह मानसिक उत्पीड़न और सामाजिक बदनामी का कारण है।
- **Drug Trafficking Online**: डार्क वेब पर अवैध वस्तुओं की बिक्री — यह अंतरराष्ट्रीय अपराध है।
- **Digital Arrest**: अपराधी खुद को पुलिस या सरकारी अधिकारी बताकर ऑनलाइन “गिरफ्तारी” का डर दिखाते हैं और ठगी करते हैं।
- **Virtual Kidnapping**: झूठा दावा करना कि किसी को अगवा कर लिया गया है और फिरौती की मांग करना।

3b. सोशल मीडिया व ऑनलाइन सुरक्षा (Social Exploitation & Cyber Safety)

✅ Do's:

- संदिग्ध या अनुचित संपर्क की तुरंत रिपोर्ट करें और ऐसे प्रोफाइल को ब्लॉक करें।
- सोशल मीडिया अकाउंट्स को निजी रखें व फर्जी खातों की रिपोर्ट करें
- फिशिंग कॉल, ईमेल या लिंक की जांच करें और अनजान लिंक पर क्लिक न करें।
- पासवर्ड बदलें, दो-कारक प्रमाणीकरण (2FA) सक्रिय करें और सबूत के लिए स्क्रीनशॉट सुरक्षित रखें।
- ब्लैकमेल या आर्थिक धोखाधड़ी की स्थिति में बैंक और साइबर सेल को तुरंत सूचित करें।

❌ Don'ts:

- अनजान व्यक्तियों के फ्रेंड रिक्वेस्ट या चैट अनुरोध स्वीकार न करें।
- बच्चों को ऑनलाइन गतिविधियों के दौरान निगरानी में रखें और उनके डर को अनदेखा न करें।
- ऑनलाइन रिश्तों में जल्दी भरोसा या वित्तीय मदद न करें।
- कभी भी व्यक्तिगत जानकारी, OTP, या फोटो/वीडियो साझा न करें।
- संदिग्ध लिंक, वेबसाइट या प्रोफाइल से दूर रहें और किसी भी ब्लैकमेल पर प्रतिक्रिया न दें।

4. भ्रामक सूचना व फर्जी कंटेंट (Fake Information & Online Manipulation)

- **फेक रिव्यू**: उत्पाद/सेवा के लिए झूठी समीक्षाएँ लिखवा कर उपभोक्ताओं को भ्रमित करना।
- **सर्च इंजन स्कैम:** फर्जी वेबसाइटों को ऊपर दिखाकर यूज़र को नकली साइट पर भटकाना।
- **IDN होमोग्राफ अटैक**: दिखने में समान नकली डोमेन बनाकर यूज़र को ठगना (URL ध्यान रखें)।
- **फेक जॉब लेटर**: नकली नौकरी/परीक्षा पत्र से पैसा या निजी जानकारी ठगना।
- **परीक्षा में अनुचित प्रथाएँ**: ऑनलाइन परीक्षाओं में चीटिंग या असामाजिक सहायता देना।

✅ Do's:

- किसी खबर पर विश्वास करने से पहले स्रोत जाँचें।सत्यापित मीडिया चैनल या सरकारी वेबसाइटों से जानकारी लें।
- नियमित रूप से सिस्टम अपडेट और सिक्योरिटी पैच लगाएँ।
- संस्थागत वेबसाइटों की सुरक्षा स्कैन करवाते रहें।

❌ Don't's:

- बिना सत्यापन खबरें शेयर न करें।
- सनसनीखेज पोस्टों को फॉरवर्ड करने से बचें।
- भावनात्मक पोस्टों पर तुरंत प्रतिक्रिया न दें।

5. Online Radicalization Crime

- **हैक्टिविज़्म**: राजनीतिक/सामाजिक संदेश के लिए वेबसाइटें हैक या डेटा लीक करना।
- **ऑनलाइन रेडिकलाइज़ेशन**: इंटरनेट पर चरमपंथी विचार फैलाकर युवाओं को भड़काना।
- **साइबर वॉरफेयर**: राष्ट्र या संगठन स्तर पर डिजिटल सिस्टम पर रणनीतिक हमले।

✅ Do's:

- एआई का उपयोग शिक्षा, अनुसंधान और सकारात्मक कार्यों के लिए करें।
- नैतिक एआई दिशानिर्देशों का पालन करें।
- ब्राउज़र और ऐड-ब्लॉकर को अपडेट रखें।

❌ Don't:

- अनधिकृत सॉफ़्टवेयर या हेकिंग टूल का इस्तेमाल न करें।
- संवेदनशील नेटवर्क तक बिना अनुमति पहुंचने की कोशिश न करें।
- निजी जानकारी कभी भी किसी अज्ञात व्यक्ति के साथ साझा न करें।