माध्यमिक शिक्षा विभाग, उत्तर प्रदेश

साइबर सुरक्षित बेटी

सतर्क,सजग,समझदार

डिजिटल युग में सुरक्षित बेटी

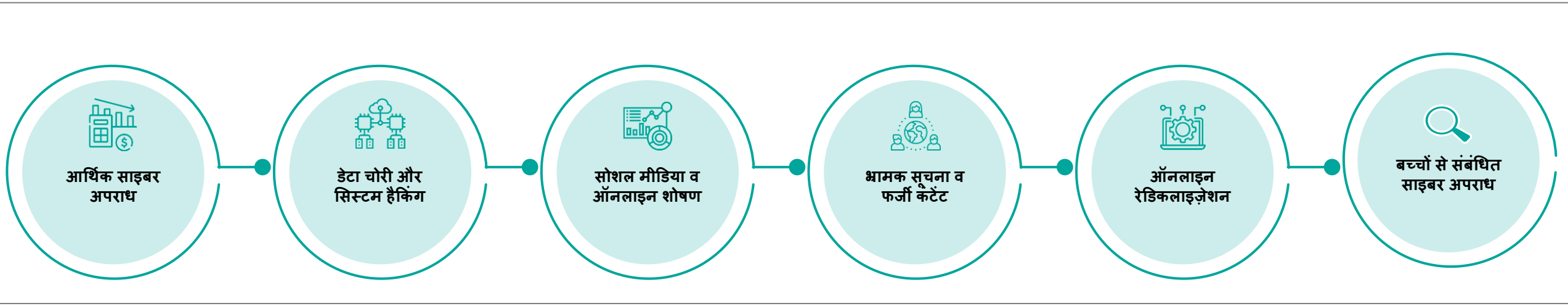
आत्मविश्वास से मुस्कुराती हमारी साइबर सुरक्षित बेटी है,
पढाई,मनोरंजन,सोशल मीडिया का जो लाभ खूब उठाती है|
पर ऑनलाइन अपराधों के खतरों से सतर्क हमेशा रहती है,
अपना हर कदम सावधानी और समझदारी से यह उठाती है|

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।

6. बच्चों से संबंधित साइबर क्राइम

- **Kids Mobile Phone Cyber Crimes:** ऐसे साइबर अपराध हैं जो बच्चों के मोबाइल फोन के माध्यम से होते हैं। इसमें ऑनलाइन ठगी, हैकिंग, साइबर बुलिंग, अप्राकृतिक कंटेंट और पहचान की चोरी शामिल हो सकते हैं। बच्चों की सुरक्षा के लिए माता-पिता और शिक्षक को मोबाइल उपयोग और इंटरनेट की निगरानी करनी चाहिए।
- **Cyber Grooming:** साइबर ग्रूमिंग एक साइबर अपराध है, जिसमें अपराधी बच्चों या नाबालिगों से ऑनलाइन दोस्ती कर उनके साथ शारीरिक या मानसिक शोषण करने की कोशिश करता है।अपराधी सोशल मीडिया, चैट एप या गेमिंग प्लेटफॉर्म पर बच्चे का भरोसा जीतकर उन्हें नुकसान पहुँचाने वाले व्यवहार की ओर ले जाता है।यह गंभीर अपराध है और बच्चों की सुरक्षा, मानसिक स्वास्थ्य और परिवार पर गहरा प्रभाव डालता हैं।

✅ Do's:

- बच्चों को ऑनलाइन मित्रता और गेम्स के खतरे बताएं।
- अपमानजनक टिप्पणी या धमकी मिलने पर स्क्रीनशॉट रखें।
- किसी फर्जी प्रोफाइल या बुलिंग की तुरंत रिपोर्ट करें।
- परिवार में "डिजिटल बातचीत" का माहौल बनाएँ।

❌ Don'ts:

- अजनबियों के मैसेज या वीडियो कॉल का तुरंत जवाब न दें।
- निजी फोटो भेजने की गलती न करें।
- ऑनलाइन गेम्स या चैट्स में अपनी असली जानकारी न दें।
- साइबर बुलिंग का जवाब गुस्से में न दें।

ये गतिविधियाँ लोगों को आर्थिक अपराधों के प्रति व्यावहारिक रूप से जागरूक करने में मदद करेंगी।

1	शपथ
2	सर्टिफिकेट ऑफ़ कम्पलीशन
3	रोल-प्ले: “सुरक्षित सोशल मीडिया” (Role-play)
4	गेम: “पासवर्ड चेलेन्ज” (Interactive Password Game)
5	क्रिएटिव प्रोजेक्ट: “साइबर सेफ्टी पोस्टर (Poster & Meme Making)
6	“संदेह सूची (Red Flag) बिंगो” खेल खेल में|
7	छोटी-सीमित कोडिंग/AI सेशन: “Prompt Safety” (LLM awareness)
8	पैरेंट/टीचर सत्र: “डिजिटल होमवर्क”
9	मिनी-चैलेंज: “डिजिटल डिटॉक्स डे”
10	पोस्टर तथा सलोगन प्रतियोगिता
11	एक छोटा उदाहरण

साइबर सुरक्षा हेतु विद्यालय स्तर पर विभिन्न गतिविधियों का आयोजन (1/4)

शपथ

“मैं शपथ लेती हूँ कि मैं सतर्क और जागरूक बन कर इंटरनेट का उपयोग जिम्मेदारी से करूँगी।
मैं अपनी पहचान, डेटा और व्यक्तिगत जानकारी सुरक्षित रखूँगी ।

मैं किसी भी फेक प्रोफ़ाइल, संदिग्ध लिंक या संदेश पर विश्वास नहीं करूँगी, सोच-समझकर सुरक्षित वेबसाइट का ही प्रयोग करूँगी।

मैं हमेशा दूसरों की गोपनीयता और सम्मान का ध्यान रखूँगी तथा कभी भी साइबर बुलिंग नहीं करूँगी और न ही उत्पीड़न ,ग़लत व्यवहार को सहन करूँगी।

मैं अपना ओटीपी /पिन किसी को नहीं बताऊँगी। मैं अपने परिवार,दोस्तों तथा सहपाठियों को भी साइबर सुरक्षित रहने के लिए जागरूक करूँगी तथा किसी भी संदिग्ध गतिविधि की सूचना हेल्पलाइन नंबर 1930 पर दूँगी।

मैं उत्तर प्रदेश की एक जागरूक, समझदार और साइबर सुरक्षित बेटी बनकर अपने प्रदेश को साइबर क्राइम मुक्त बनाने में सक्रिय योगदान दूँगी।

साइबर सुरक्षा हेतु विद्यालय स्तर पर विभिन्न गतिविधियों का आयोजन (2/4)

गेम: "पासवर्ड चेलेन्ज" (Interactive Password Game)

उद्देश्य: मजबूत पासवर्ड तैयार करना। कार्य योजना-

- पासवर्ड के घटक (अपर केस, लोअर केस, नंबर, सिंबल, लंबाई) के कार्ड दिखाएँ।
- दो टीमों में मुकाबला: किस टीम का सदस्य 60 सेकंड में सबसे मजबूत, याद रखने योग्य पासवर्ड बना पाएगा?

प्रत्येक पासवर्ड की स्टोरी बनवाएँ — याद रखने के लिए।

निष्कर्ष-पासवर्ड लंबा, मिश्रित और यूनिक रखें। पासवर्ड मैनेजर की भूमिका शिक्षिका निभाएगी।

वर्कशॉप: "फेक न्यूज़ पहचान" (Fake News Detective)

उद्देश्य: स्रोत सत्यापन, तथ्य-जांच। प्रिंटेड न्यूज क्लिप्स (मिश्रित असली/नकली) बाँटें — छात्राओं को 4–5 मिनट में पहचान करनी है। शिक्षिका चेकलिस्ट अपने पास रखेगी।

- चेकलिस्ट दें: स्रोत, तारीख, लेखक, लिंक, दूसरे स्रोतों से मिलान।
- हर समूह अपना निष्कर्ष क्लास को बताए — और बताए कि वे किस बिंदु पर शक करते हैं।

निष्कर्ष-खबरें शेयर करने से पहले क्रॉस-चेक करें; स्क्रिनशॉट + स्रोत शेयरिंग न करें।

रोल-प्ले: "सुरक्षित सोशल मीडिया" (Role-play)

उद्देश्य: पहचानना — निजी जानकारी क्या है, कैसे संभालें। सामग्री: कार्ड पर परिदृश्य (scenario), जाँच सूची (checklist)।

कार्य योजना-

- छात्राओं को 4–5 की टुकड़ियों में बाँटें।
- हर समूह को एक परिदृश्य कार्ड दें (उदा. "एक अजनबी दोस्त बनाता है", "फेक इन्फ्लुएंसर पैसे माँगता है")।
- कोई भी 5 मिनट्स की स्किट।
- क्लास डिस्कशन: क्या सही/गलत हुआ? क्या करें/क्या न करें?

सीख: निजी जानकारी न दें, दोस्ती/संदेश को सत्यापित करें, रिपोर्ट करें। शिक्षिका मार्गदर्शक बनेगी।

साइबर सुरक्षा हेतु विद्यालय स्तर पर विभिन्न गतिविधियों का आयोजन (3/4)

क्रिएटिव प्रोजेक्ट: "साइबर सेफ्टी पोस्टर (Poster & Meme Making)

उद्देश्य: संदेश रचनात्मक रूप से फैलाना। कार्य योजना - थीम दें: "5 साइबर सेफ्टी नियम"।

- टीम बनाकर पोस्टर बनवाएँ।
- सबसे प्रभावी पोस्टर की प्रदर्शनी और पुरस्कार देकर प्रोत्साहित करे।
- निष्कर्ष-प्रमुख नियम (Do's) के पोस्टर विद्यालय में कक्षा कक्ष में लगवाएगी ताकि सभी तक पहुंच बढ़ सके।

रोल-प्ले: "कॉल मर्ज/वॉइस फ्रॉड" सिमुलेशन

उद्देश्य: कॉल-आधारित स्कैम पहचानना।

- एक छात्रा 'स्कैमर' और एक बच्ची 'अभिभावक' बने।
- स्कैमर तुरंत पैसे माँगने की तकनीक दिखाए। जैसे आपके द्वारा पासपोर्ट के लिए आवेदन किया है इस लिंक पर फ़ीस भेजे।
- क्लास सुझाव दे कि सुरक्षित प्रतिक्रिया क्या होगी (कौन-कौन कॉल करें, बैंक से कैसे चेक करें)।

सीख: कॉल पर जानकारी न दें; बैंक से सत्यापन आवश्यक; ग्राहक सेवा नंबर का उपयोग करें।

गतिविधि: "संदेह सूची (Red Flag) बिंगो" खेल खेल में|

उद्देश्य: धोखाधड़ी की लाल-झंडियाँ पहचानना।

कार्य योजना -

- बिंगो कार्ड (फेक लिंक, अजनबी अनुरोध, जल्दबाजी वाले संदेश आदि)। करें।
- टीचर कॉल में परिदृश्य पढ़ते हैं; खिलाड़ी चिह्नित करें।
- पहले "बिंगो" वाली छात्रा जीतती है—और वह यह भी बताएगी कि यह किस प्रकार धोखाधड़ी की गई है|

निष्कर्ष-टीम भवन के साथ सतर्कता, साझा ज्ञान।

छोटी-सीमित कोडिंग/AI सेशन: "Prompt Safety" (LLM awareness)

उद्देश्य: AI से सुरक्षित बातचीत, निजी जानकारी न देना।

कार्य योजना

- सरल उदाहरण दिखाएँ — क्या न पूछें (PAN, passwords)।
- छात्राओं से "सुरक्षित प्रश्न" बनवाएँ।
- AI से आने वाली सलाह को क्रॉस-चेक करने की आदत सिखाएँ।

सीख: AI से सावधानी, प्रॉम्प्ट में संवेदनशील जानकारी शामिल न करें।

साइबर सुरक्षा हेतु विद्यालय स्तर पर विभिन्न गतिविधियों का आयोजन (4/4)

पैरेंट/टीचर सत्र: "डिजिटल होमवर्क"

उद्देश्य: घर-परिवार में नियम बनाना।

- स्कूल में किए गए एक्टिविटीज साझा करें।
- घरेलू नियम: स्क्रीन टाइम, ऐप पर नियंत्रण, रिपोर्टिंग नियम बनवाएँ।
- अभिभावकों से संवाद कर उन्हें भी साइबर अपराधों से अवगत कराना ताकि हमारी बेटियाँ सुरक्षित रहे ।
- निष्कर्ष-घर और स्कूल का समन्वय ज़रूरी।

पोस्टर तथा सलोगन प्रतियोगिता

- 'हमेशा सोर्स वेरिफाई करो — शेयर करने से पहले 2 बार सोचो।
- "पासवर्ड लंबा और यूनिक रखें — किसी से साझा न करें।
- "अज्ञात लिंक पर क्लिक न करें — पहले पूछें।
- "संदिग्ध कॉल/मैसेज पर पैसे न भेजें — बैंक से स्वयं पुष्टि करें।
- "किसी भी खतरे को स्कूल/अभिभावक/पुलिस को रिपोर्ट करें।
- 'हेल्पलाइन नंबर 1930 हमेशा याद रखें '

मिनी-चैलेंज: "डिजिटल डिटॉक्स डे"

उद्देश्य: स्क्रीन-हैबिट समझना।

कार्य योजना-

- एक दिन के लिए सोशल मीडिया बंद।
- ऑफ़लाइन गतिविधियाँ — ग्रुप रीडिंग/हाथ से कला।
- दिन के अंत में अनुभव साझा करें: क्या बेहतर महसूस हुआ?

निष्कर्ष-मानसिक स्वास्थ्य, निर्भरता की समझ।

रोल-प्ले स्क्रिप्ट (एक छोटा उदाहरण)

अपराधी: "बैंक से बोल रहा हूँ, OTP दो।"छात्रा: "कौन? मैं बैंक से पूछती हूँ।" अपराधी दबाव डालता है, छात्रा आधिकारिक नंबर पर कॉल कर पुष्टि करती है। अपराधी हारकर फोन काट देता है।

सुरक्षा:

- निजी जानकारी न दें।
- मजबूत पासवर्ड और 2FA रखें।
- संदिग्ध लिंक न खोलें।
- साइबर पुलिस को रिपोर्ट करें।
- माता-पिता से बात करें और नियम बनाएं।

स्लोगन और साइबर क्राइम हेल्पलाइन

"आज की लड़की सिर्फ स्मार्टफोन नहीं चलाती,
वह डिजिटल दुनिया को समझदारी से चलाना भी जानती है —
वही है साइबर सेफ बेटी।"
"इंटरनेट ने हमारी दुनिया को जोड़ दिया है,लेकिन सुरक्षा के धागे को मजबूत रखना हर छात्रा की जिम्मेदारी
साइबर सेफ बेटी वह है जो ऑनलाइन दुनिया में अपनी पहचान, गोपनीयता और मर्यादा-
तीनों को सुरक्षित रखती है।"
डिजिटल युग में स्मार्ट वही नहीं जो तकनीक जानता है,
बल्कि वह जो उसे सुरक्षित रूप से उपयोग करना जानता है।
"साइबर सुरक्षा कोई विकल्प नहीं,यह हर आधुनिक छात्रा की पहचान है।"
"जैसे सड़क पर ट्रैफिक नियम जरूरी हैं,वैसे ही इंटरनेट पर साइबर नियम जरूरी हैं।"
"एक समझदार क्लिक आपकी सुरक्षा बढ़ा सकता है,
एक गलत क्लिक नुकसान पहुँच सकता है —
इसलिए बनिए Cyber Safe Beti"

साइबर क्राइम में हमारे मददगार-
राष्ट्रीय साइबर हेल्पलाइन नंबर-1930
www.cybercrime.gov.in ऑनलाइन शिकायत हेतु ।

वित्तीय- धोखाधड़ी- लघु नाटिका

डेबिट कार्ड क्लोनिंग

उपशीर्षक: “डिजिटल दुनिया में सतर्कता ही सबसे बड़ा सुरक्षा कवच है।”
अवधि: 4–5 मिनट
पात्र:

- काकुल – छात्रा
- सलोनी – सहपाठी
- साइबर अपराधी
- सविता मैडम – शिक्षिका
- साइबर पुलिस अधिकारी

दृश्य 1 – स्कूल का कंप्यूटर लैब

(काकुल और सलोनी ऑनलाइन गेम खेल रहीं हैं)
काकुल: वाह सलोनी, इस गेम में तो असली पैसे का इनाम मिल रहा है!
सलोनी: हाँ, लेकिन यह लिंक थोड़ा अजीब लग रहा है, लिखा है “डिटेल्स डालो और जीत पक्की।”
काकुल (जल्दबाजी में): मैं अपना कार्ड नंबर डाल देती हूँ।
(काकुल डिटेल डालती है, स्क्रीन ब्लैंक हो जाती है)
काकुल: अरे! मेरा अकाउंट तो बंद हो गया!
साइबर अपराधी (फोन पर हँसते हुए): हा हा हा! कार्ड क्लोन हो गया — अब पैसे मेरे खाते में!

दृश्य 2 – अगले दिन स्कूल में

(काकुल रोती हुई आती है)
काकुल: मेरे अकाउंट से पैसे कट गए!
सलोनी: यही तो साइबर क्राइम है काकुल! किसी भी वेबसाइट पर अपनी जानकारी नहीं डालनी चाहिए।
सविता मैडम: बच्चों, यही वजह है कि साइबर सुरक्षा की जानकारी ज़रूरी है।
काकुल: मैडम, अब क्या करूँ?
सविता मैडम: तुरंत साइबर हेल्पलाइन 1930 पर कॉल करो और रिपोर्ट दर्ज कराओ।

दृश्य 3 – साइबर पुलिस स्टेशन

साइबर अधिकारी: चिंता मत करो बेटा, हमने अपराधी की लोकेशन ट्रेस कर ली है — वह *कूच बिहार* से साइबर ठगी कर रहा है।
(अपराधी पकड़ा जाता है)
अपराधी: माफ कर दो, अब कभी ऐसा नहीं करूँगा।
काकुल: मैंने एक गलती से सीखा – ऑनलाइन जानकारी साझा करना खतरनाक है।
#समापन
सभी मिलकर:
“साइबर स्मार्ट बनो, सुरक्षित रहो!”
संदेश:
“डिजिटल दुनिया में सतर्कता ही सबसे बड़ा सुरक्षा कवच है।”
समाप्त

सीख और संदेश

✅ Do’s

- किसी भी संदिग्ध लिंक पर भरोसा न करो।
- पासवर्ड और OTP कभी शेयर न करो।
- संदिग्ध संदेश तुरंत माता-पिता या शिक्षक को बताओ।

❌ Don'ts

- वेबसाइट लिंक ध्यान से देखे बिना जानकारी न भरो।
- हर संदेश या कॉल पर विश्वास न करें।