न्याय विभाग
DEPARTMENT OF
JUSTICE

साइबर क्राइम

विधि मित्रों के माध्यम से ग्राम पंचायतों में कानूनी सशक्तिकरण

परियोजना का शीर्षक

विधि मित्रों के माध्यम से ग्राम पंचायतों में कानूनी सशक्तिकरण

1. परिचय :

साइबर क्राइम पर महत्वपूर्ण प्रशिक्षण मॉड्यूल ''विधि मित्र के माध्यम से 700 गांवों के पंचायत की कानूनी सशक्तिकरण'' परियोजना का हिस्सा है, जो बिहार लोक प्रशासन और ग्रामीण विकास संस्थान (बी.आई.पी.ए.आर.डी) द्वारा प्रारंभ की गई है। यह मॉड्यूल साधारण उद्देश्य को पूरा करने के लिए सार्वजनिक नोटिस करके निर्धारित जिलों में काम करने वाले हितधारकों को आवश्यक ज्ञान और कौशल प्रदान करके साइबर क्राइम के मुद्दे का प्रभावी रूप से सामना करने का उद्देश्य रखता है। इन हितधारकों के जागरूकता को बढ़ाकर और क्षमता को मजबूत करके, यह मॉड्यूल ग्रामीण क्षेत्रों में एक सुरक्षित और सुरक्षित डिजिटल वातावरण को बढ़ावा देने के समग्र उद्देश्य में योगदान करने का प्रयास करता है।

2. मॉड्यूल के उद्देश्य :

- कंप्यूटर अपराध के बारे में जागरूकता फैलाने और इसके विभिन्न रूपों के साथ, विशेष रूप से महिलाओं, बच्चों और ग्रामीण गांवों में

रहने वाले व्यक्तियों के सामने आने वाली चुनौतियों पर ध्यान केंद्रित करने के लिए एक पहल करना है।

- समाज पर साइबरक्राइम के प्रभाव के बारे में प्रशिक्षण देना, विशेष रूप से अश्लीलता, यौन अपराध, हिंसा, जालसाजी, वित्तीय धोखाधड़ी, पहचान चोरी और अनुचित गतिविधियों की महिमार्चना के संबंध में प्रतिभागियों को शिक्षित करना।
- सहभागियों को साइबर धोखाधड़ी और हमलों से सुरक्षा प्राप्त करने के तरीके और रणनीतियों के साथ खुद और अपने परिवार की सुरक्षा प्रदान करने के लिए।
- साइबर दुनिया में सही और गलत गतिविधियों के बीच भेदभाव करने और अपनी समुदायों में एक सुरक्षित डिजिटल संस्कृति को प्रोत्साहित करने के लिए प्रतिभागियों को सशक्त बनाना।
- साइबर क्राइम को प्रभावी तरीके से निपटने के लिए हितधारकों के बीच सहयोग और सूचना साझा करने को बढ़ावा देना।

3. मॉड्यूल की रूपरेखा :

I. साइबर क्राइम का परिचय :

a. साइबर क्राइम की परिभाषा और प्रकार – साइबर क्राइम का अर्थ होता है वे अपराध जो इंटरनेट, कंप्यूटर और अन्य इलेक्ट्रॉनिक माध्यमों का उपयोग करके किए जाते हैं। ये अपराध आपकी

व्यक्तिगत और आर्थिक सुरक्षा को प्रभावित कर सकते हैं। साइबर क्राइम के कुछ प्रमुख प्रकार हैं : ऑनलाइन धोखाधड़ी, आपत्तिजनक संदेशों का प्रसार, वेबसाइटों के अवैध उपयोग, ऑनलाइन आपराधिकता और इंटरनेट पर व्यक्तिगत जानकारी की चोरी।

b. **साइबर क्राइम का व्यक्तियों, परिवारों और समाज पर प्रभाव** – साइबर क्राइम व्यक्तियों, परिवारों और समाज पर गंभीर प्रभाव डाल सकता है। इससे आपके परिवार की सुरक्षा, आपकी व्यक्तिगत जानकारी और आपके आर्थिक हित को खतरा हो सकता है। साइबर क्राइम आपको धोखे से ग्रस्त कर सकता है, आपकी वेबसाइट या सोशल मीडिया खाते को हैक कर सकता है और आपकी व्यक्तिगत चित्रा और सम्मान को नुकसान पहुंचा सकता है।

c. **साइबर दुनिया और अश्लीलता, यौन अपराध, हिंसा और अनुचित गतिविधियों के उदय के बीच संबंध का अध्ययन** – साइबर दुनिया और अश्लीलता, यौन अपराध, हिंसा और अनुचित गतिविधियों के उदय के बीच संबंध का अध्ययनरू साइबर दुनिया अश्लीलता, यौन अपराध, हिंसा और अनुचित गतिविधियों के बढ़ने के साथ संबंधित है। इंटरनेट और सोशल मीडिया के माध्यम से लोग ऐसी अश्लीलता, यौन अपराध और हिंसा को बढ़ावा देते हैं जो समाज के लिए हानिकारक हो सकती है। इसलिए साइबर क्राइम के खिलाफ लड़ाई में यह बहुत महत्वपूर्ण है कि हम सभी एकजुट हों और ऐसे अनुचित गतिविधियों का विरोध करें।

d. **साइबर क्राइम में उभरती रुझानों और चुनौतियों का**

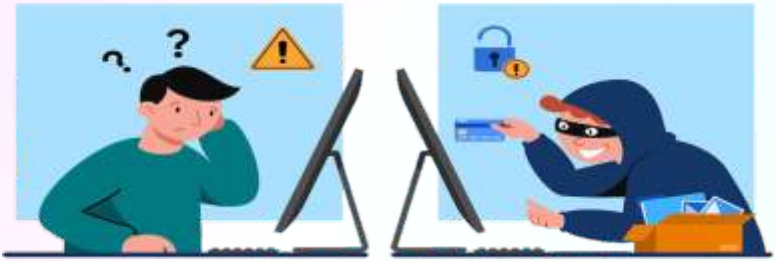
विश्लेषण – साइबरक्राइम में उभरती रुझानें और चुनौतियाँ बढ़ रही हैं। अब लोग अधिक से अधिक इंटरनेट और डिजिटल माध्यमों का उपयोग कर रहे हैं, इसलिए साइबरक्राइम की धारणा और रोकथाम बड़ी चुनौतियों का सामना कर रही है। लेकिन हम सब मिलकर इसे रोक सकते हैं और सुरक्षित इंटरनेट उपयोग कर सकते हैं। यह हमारे सभी के लिए महत्वपूर्ण है क्योंकि हम सभी अपने और अपने परिवार की सुरक्षा की जिम्मेदारी उठा सकते हैं।

II. साइबर सुरक्षा के मूलतत्व :

a. डिजिटल युग में साइबर सुरक्षा का महत्व – गांव के लोगों के लिए यह महत्वपूर्ण है कि हम समझें कि डिजिटल युग में साइबर सुरक्षा क्यों जरूरी है। आजकल हम सभी अपने मोबाइल फोन, कंप्यूटर और इंटरनेट का

उपयोग करते हैं, लेकिन इसके साथ ही हमें ध्यान देने की जरूरत है कि हमारी निजी जानकारी और डेटा सुरक्षित रहें। साइबर सुरक्षा हमें इंटरनेट पर चोरी या आपत्तिजनक गतिविधियों से बचाती है। यह हमारी सुरक्षा और निजीता की रक्षा करने में मदद करती है।

b. **सामान्य साइबर धमकियों और कमजोरियों** – यह आवश्यक है कि हम गांव के लोग सामान्य साइबर



धमकियों और कमजोरियों के बारे में जानें। ये धमकियां हमारे डिजिटल जीवन को प्रभावित कर सकती हैं, जैसे आपत्तिजनक मैसेज, फ़र्ज़ी ईमेल, और ऑनलाइन धोखाधड़ी। हमें इन धमकियों से बचने के लिए सतर्क रहना चाहिए और इंटरनेट पर सुरक्षित रहने के तरीकों को समझना चाहिए।

c. **डिजिटल उपकरणों और नेटवर्क की सुरक्षा के लिए सर्वश्रेष्ठ अभ्यास** – गांव के लोगों के लिए यह जानना जरूरी है कि हमें अपने डिजिटल उपकरणों और नेटवर्क की सुरक्षा के लिए सर्वश्रेष्ठ अभ्यास करने की आवश्यकता होती है। हमें मजबूत पासवर्ड बनाना, अद्यतन रखना और अद्यतन रखने के लिए अच्छे एंटीवायरस सॉफ़्टवेयर का उपयोग करना चाहिए। इसके साथ ही हमें गैरजरूरी ऐप्स और वेबसाइटों का उपयोग न करना चाहिए जो

हमारे डेटा को चोरी कर सकते हैं। हमें अपने परिवार और आपसी सहयोग के माध्यम से एक सुरक्षित डिजिटल वातावरण बनाने के लिए इन अभ्यासों को अपनाना चाहिए।

III. महिलाओं और बच्चों को निशाना बनाने वाले साइबर खतरे :

a. महिलाओं और बच्चों को निशाना बनाने वाले साइबर खतरे – गांव के लोगों को समझाने के लिए हमें यह जानना आवश्यक है कि साइबर खतरों में महिलाएं और बच्चे अधिक विपरीत रूप से प्रभावित होते हैं। इसका कारण है कि वे इंटरनेट के उपयोग को अच्छी तरह से समझने और सुरक्षित रखने की ज्ञान और संपूर्ण जागरूकता की कमी के कारण खतरे के निशान बन सकते हैं। हमें इन साइबर खतरों को पहचानने और उनसे

बचने के तरीके को सीखने की आवश्यकता है ताकि हमारी महिलाएं और बच्चे सुरक्षित रह सकें।

b. **सेक्सटिंग और गैर–सहमति से गहरी संवेदनशील सामग्री का साझा करना (प्रतिशोध पोर्न)** – साइबर दुनिया में यह भी एक खतरा है कि कुछ लोग बिना अनुमति के लोगों के बीच गहरी संवेदनशील सामग्री जैसे कि गैर–सहमति से सेक्सटिंग (सेक्स की फोटो और वीडियो) या प्रतिशोध पोर्न (गलत तरीके से इस्तेमाल होने वाली संभोगशृंगारिक सामग्री) को साझा कर सकते हैं। हमें इस तरह के अपराधों को पहचानने और इससे बचने के उपायों को सीखने की जरूरत है।

c. **ऑनलाइन हरासमेंट और ट्रैकिंग** – ऑनलाइन हरासमेंट एक और बड़ा समस्या है जो हमें समझनी चाहिए। कुछ लोग इंटरनेट का दुरुपयोग करके दूसरों को परेशान कर सकते हैं और उनका पीछा कर सकते हैं। हमें ऐसे हरासमेंट को पहचानने और उनसे बचने के तरीके को सीखने की जरूरत है।

d. **ग्रूमिंग और बाल शोषण** – एक और गंभीर समस्या है जिसे हमें समझना होगा वह है ग्रूमिंग और बाल शोषण। कुछ लोग इंटरनेट का उपयोग करके बच्चों को लक्ष्य बना सकते हैं और उन्हें ठग सकते हैं। हमें इस तरह के अपराधों को पहचानने और इससे बचने के तरीके को सीखने की आवश्यकता है।

e. **पहचान चोरी, अनुकरण और महिलाओं और बच्चों को लक्ष्य बनाने वाला धोखाधड़ी** – इंटरनेट पर कुछ लोग धोखाधड़ी करके हमारी पहचान चुरा सकते हैं, हमें नकली वेबसाइटों और खतरनाक लिंक्स से बचना चाहिए। वे महिलाओं और बच्चों को लक्ष्य बनाकर उन्हें ठग सकते हैं। हमें इन धोखाधड़ी के तरीकों को पहचानने और उनसे बचने की जरूरत है।

f. **महिलाओं को लक्ष्य बनाने वाले वित्तीय धोखाधड़ी और ठगी** – कुछ लोग महिलाओं को वित्तीय धोखाधड़ी करके और उनसे ठगी करके लाभ उठाते हैं। ऐसी स्थिति में, आपको सतर्क रहना चाहिए और ऐसे लोगों से सावधान रहना चाहिए जो आपसे वित्तीय जानकारी मांगते हैं।

g. **ऑनलाइन डेटिंग धोखाधड़ी** – ऑनलाइन डेटिंग में धोखाधड़ी का खतरा भी होता है। आपको यह सुनिश्चित करना चाहिए कि आप विश्वसनीय और सत्यापित व्यक्ति

के साथ ही अपनी जानकारी साझा करते हैं और वे व्यक्ति आपके लिए सुरक्षित हों।

h. **साइबर बुलिंग और साइबर अपमान** – ऑनलाइन माध्यम में बुलिंग और अपमान एक अन्य बड़ा मुद्दा है। लोग आपको आपत्तिजनक टिप्पणियां कर सकते हैं या आपको बुरे ढंग से बोल सकते हैं। यह आपके लिए मानसिक रूप से क्षतिपूर्ति कर सकता है। आपको ऐसे मामलों में सुरक्षित रहना चाहिए और इसे रिपोर्ट करना चाहिए।

I. **डोक्सिंग (ऑनलाइन प्राइवेट जानकारी प्रकाशित करना)** – डोक्सिंग (ऑनलाइन प्राइवेट जानकारी प्रकाशित करना) : डोक्सिंग एक और साइबर खतरा है जहां लोग आपकी निजी जानकारी को ऑनलाइन शेयर करते हैं। यह बहुत ही गलत होता है और इससे आपके जीवन पर बहुत बड़ा प्रभाव पड़ सकता है। आपको अपनी निजी जानकारी की सुरक्षा करनी चाहिए और ऐसे लोगों को बताना चाहिए कि ऐसा करना गलत है।

यह सभी साइबर खतरे हमारे लिए खतरनाक हो सकते हैं, खासकर गांव के महिलाओं और बच्चों के लिए। हमें सभी इस बात का महत्व समझना चाहिए और यह सुनिश्चित करना चाहिए कि हम अपनी सुरक्षा के लिए आवश्यक कदम उठाते हैं। साइबर अपराधों से बचने के लिए सहयोग, जागरूकता, और ज्ञान का महत्व हमें समझाना चाहिए ताकि हम एक सुरक्षित और सदर डिजिटल संस्कृति का निर्माण कर सकें।

IV. बच्चों और माता–पिता के लिए साइबर सुरक्षा :

a. माता–पिता के नियंत्रण और मॉनिटरिंग उपकरण – आपके बच्चों की सुरक्षा के लिए आपको उनकी गतिविधियों को निगरानी करने और नियंत्रित करने के उपाय करने चाहिए। इससे आप उनके ऑनलाइन संसार में क्या हो रहा है के बारे में जान सकेंगे।

b. ऑनलाइन सुरक्षा और जिम्मेदार इंटरनेट उपयोग के बारे में बच्चों को सिखाना – बच्चों को समझाना महत्वपूर्ण है कि वे इंटरनेट का सही और जिम्मेदारीपूर्ण तरीके से उपयोग करें। उन्हें बताएं कि कैसे अपनी पर्सनल जानकारी को सुरक्षित रखें, अज्ञात लोगों के साथ संवाद न करें और अनुचित सामग्री से दूर रहें।

c. बच्चों के साथ ऑनलाइन अनुभवों के बारे में खुले संवाद के माध्यम स्थापित करना – बच्चों को

आपके साथ खुले मन से बातचीत करने के लिए प्रोत्साहित करें। उन्हें बताएं कि यदि उन्हें किसी ऑनलाइन संदेश या साइट में कुछ अनुचित या चोटिल सामग्री दिखाई दे तो वे तुरंत आपको बताएं। यह उन्हें सुरक्षित और आपके साथ संवाद करने में सक्षम बनाएगा।

d. माता–पिता को संभावित खतरों और चेतावनी चिह्नों के बारे में शिक्षित करना – माता–पिता को समझना आवश्यक है कि ऑनलाइन दुनिया में कौन से खतरे हो सकते हैं और उनकी पहचान कैसे करें। उन्हें बताएं कि किसी अज्ञात लिंक पर क्लिक करने, अनचाहे ईमेल या संदेश को खोलने या व्यक्तिगत जानकारी साझा करने से बचें। इससे उनकी और उनके परिवार की सुरक्षा सुनिश्चित होगी। माता–पिता को संभावित साइबर खतरों के बारे में जागरूक होना चाहिए और उन्हें अपने बच्चों को इन खतरों के चेतावनी चिह्नों के बारे में सिखाना चाहिए।

इस तरीके से, आप गांव की जनता के लिए साइबर सुरक्षा के महत्व को सरल और समझने योग्य ढंग से समझा सकते हैं। इससे उन्हें उसकी महत्वाकांक्षा और योग्यता की समझ होगी।

V. साइबर अपराधों के निवारण और सुरक्षा के तरीके :

a. पासवर्ड प्रबंधन और मजबूत प्रमाणीकरण – अपने खातों को सुरक्षित रखने के लिए, हमें अपने पासवर्डों का सही प्रबंधन करना चाहिए। अच्छे और मजबूत पासवर्ड चुनें।

b. सुरक्षित इंटरनेट ब्राउज़िंग और सोशल मीडिया

अभ्यास – इंटरनेट का सही और सुरक्षित इस्तेमाल करना अत्यंत महत्वपूर्ण है। अनचाहे साइबर खतरों से बचने के लिए सतर्क रहें, अज्ञात लिंक्स पर क्लिक न करें और अपनी निजी जानकारी को सोशल मीडिया पर न शेयर करें।

c. **गोपनीयता सेटिंग्स और ऑनलाइन व्यक्तिगत जानकारी का नियंत्रण** – अपनी ऑनलाइन गोपनीयता की सेटिंग्स को समझें और नियंत्रण में रखें। अपनी व्यक्तिगत जानकारी को ज्यादा साझा न करें और केवल विश्वसनीय वेबसाइट्स पर ही दाखिल करें।

d. **फिशिंग और सोशल इंजीनियरिंग हमलों की पहचान और टालना** – धोखाधड़ी के खिलाफ सतर्क रहें और फिशिंग या सोशल इंजीनियरिंग के हमलों को पहचानें। ऐसे हमलों से बचने के लिए, आपको अज्ञात संदेशों, आगंतुक अनुरोधों, या संदिग्ध वेबसाइट्स से सतर्क रहना चाहिए।

e. **व्यक्तिगत उपकरणों और होम नेटवर्क की सुरक्षा** – अपने व्यक्तिगत उपकरणों और होम नेटवर्क की सुरक्षा को

मजबूत बनाना आवश्यक है। सुरक्षा सॉफ़्टवेयर का उपयोग करें, नेटवर्क को पासवर्ड से सुरक्षित करें, और अपने डिवाइसेज़ को सुरक्षित स्थान पर रखें।

ये तरीके गांव के लोगों के लिए सरल और समझने में आसान हैं। साथ ही, इनका उद्देश्य गांव के लोगों को सुरक्षा की महत्वता को समझाना और उन्हें इन तरीकों के माध्यम से संज्ञान और सुरक्षा की बढ़ती हुई जरूरत को आसानी से समझने में मदद करना है।

VI. साइबर नीति और जिम्मेदार इंटरनेट उपयोग :– गांव के लोगों को बहुत ही आसान और समझने योग्य तरीके से समझाने के लिए, निम्नलिखित विवरण में साइबर नीति और जिम्मेदार इंटरनेट उपयोग के महत्व को संबंधित बनाया गया है। गांव के लोगों के लिए यह जरूरी है कि वे इंटरनेट का जिम्मेदारीभर उपयोग करें। यह कुछ महत्वपूर्ण बातें हैं जो आपको समझने में मदद करेंगी :

a. **ऑनलाइन में जिम्मेदार व्यवहार को बढ़ावा देना –** आपको इंटरनेट पर सभ्यता के साथ बर्ताव करना चाहिए। आपको दूसरों के साथ आदरपूर्वक व्यवहार करना चाहिए और किसी को भी चोट नहीं पहुंचाना चाहिए।

b. **डिजिटल नागरिकता और सम्मानपूर्ण संचार की शिक्षा देना –** आपको सीखना चाहिए कि कैसे आप इंटरनेट का उपयोग करके एक अच्छे नागरिक बन सकते हैं। आपको अपने माता–पिता और सभी वरिष्ठ लोगों के साथ सम्मानपूर्ण ढंग से बात करना चाहिए।

c. **ऑनलाइन जानकारी का मूल्यांकन करने के लिए समीक्षात्मक सोच को प्रोत्साहित करना –** जब आप इंटरनेट पर कोई जानकारी पढ़ते हैं, तो आपको इसकी सत्यता और महत्वाकांक्षा को जांचने की आवश्यकता होती है। ऐसा करने से आप आपके लिए सही जानकारी को अलग कर सकते हैं और गलत जानकारी से बच सकते हैं।

d. **साइबर बुलींग और उत्पीड़न की रिपोर्टिंग और समस्या का समाधान करना –** यदि आपको किसी ने इंटरनेट पर परेशान किया है या आपको किसी समस्या का सामना करना पड़ रहा है, तो आपको इसे रिपोर्ट करना चाहिए। आपको समाधान की सहायता के लिए संबंधित अधिकारीयों और नेटवर्क के संचालकों के पास जाना चाहिए।

इन उपायों का पालन करने से आप और आपका परिवार सुरक्षित रहेंगे और इंटरनेट के साथ स्वच्छ और सुरक्षित डिजिटल वातावरण का निर्माण करेंगे।

VII. साइबर अपराध कानून और विनियमन :

a. **संबंधित राष्ट्रीय कानूनों का संक्षेप में अवलोकन –** साइबर अपराध के बारे में कानून और नियमों की बात करेंगे। साइबर अपराध वाले कानूनों का मतलब है कि जिन अपराधियों ने इंटरनेट और डिजिटल दुनिया में ग़ैरकानूनी काम किए हैं, उनके ख़िलाफ़ कानून और नियम बनाए गए हैं। ये कानून देश के अंदर और बाहर से जुड़े हो सकते हैं। इन कानूनों के माध्यम से साइबर अपराधियों को सज़ा दी जाती है ताकि लोग सुरक्षित रह सकें और ऐसे अपराधों से बच सकें।

b. **कानूनी ढांचे और अधिकारिक क्षेत्रों की समझ –** अब हम बात करेंगे कानूनी ढांचे और अधिकारिक क्षेत्रों की। जब कोई अपराधी ग़ैरकानूनी काम करता है, तो साइबर पुलिस और न्यायिक संरचना इसे ज़िम्मेदारी बनाती है। वे इस प्रक्रिया में शामिल होकर अपराधी को

ज़ालिमाना कार्रवाई करते हैं। कानूनी ढांचे और अधिकारिक क्षेत्रों की समझ वाले लोग इन संरचनाओं को चला कर लोगों को सुरक्षित रखने में मदद करते हैं। ये संरचनाएँ हमारी सरकार द्वारा निर्मित की जाती हैं ताकि हम सब सुरक्षित रह सकें।

c. साइबर अपराधों के निवारण और दण्डाधिकार के स्तरों में हिस्सेदारों की भूमिका और जिम्मेदारियाँ – आप सब ने साइबर अपराधों के निवारण और दण्डाधिकार के बारे में सुना होगा। ये बात बहुत महत्वपूर्ण है क्योंकि इसके माध्यम से हम साइबर अपराधों के ख़िलाफ़ लड़ाई लड़ सकते हैं। साइबर पुलिस, कोर्ट और सरकार इस लड़ाई में हमारे साथी हैं और उनकी ज़िम्मेदारियाँ हैं कि हमें सुरक्षित रखें। इन स्तरों में हिस्सेदारों की भूमिका यह होती है कि वे अपराधियों को पकड़ने और सज़ा देने में सहायता करते हैं। हमारी सुरक्षा के लिए ये बहुत आवश्यक है और हमें इसे समझना चाहिए।

VIII. मोबाइल उपकरणों के लिए साइबर सुरक्षा :

a. सुरक्षित ऐप स्थापना और अनुमतियों – आपके मोबाइल में उन्नत सुरक्षा ऐप्स को स्थापित करना और अपने डेटा तक पहुँच को संगठित रखने के लिए जरूरी है। इससे आपकी व्यक्तिगत जानकारी सुरक्षित रहती है।

b. **मोबाइल मैलवेयर और धोखाधड़ी से बचाव** – सावधान रहें, क्योंकि मोबाइल में वायरस और धोखेबाजी की संभावना होती है। इसलिए, अपराधियों से बचने के लिए अद्यतन अच्छी सुरक्षा सॉफ़्टवेयर का उपयोग करें।

c. **स्मार्टफोन और टैबलेट पर व्यक्तिगत डेटा की सुरक्षा** – अपने स्मार्टफोन और टैबलेट पर रखे गए व्यक्तिगत जानकारी को सुरक्षित रखने के लिए पासवर्ड या पिन का उपयोग करें। इससे आपकी प्राइवेसी सुरक्षित रहेगी।

d. **मोबाइल भुगतान ऐप और लेन–देन की सुरक्षा** – मोबाइल भुगतान ऐप का उपयोग करने से पहले, यह सुनिश्चित करें कि ऐप सुरक्षित है और आपके लेन–देन की सुरक्षा का ध्यान रखती है। आपके पैसे की सुरक्षा बहुत महत्वपूर्ण है।

e. **मोबाइल उपकरण के ट्रैकिंग और दूरस्थ हटाने के सुविधाओं का उपयोग करें** – अपने मोबाइल को खोने की स्थिति में, ट्रैकिंग सुविधा का उपयोग करके उसे ढूंढ़

सकते हैं और उसे दूरस्थ कर सकते हैं। इससे आपका मोबाइल सुरक्षित रहेगा और अनचाहे हाथों में नहीं पड़ेगा।

उपरोक्त सुरक्षा उपायों का अपनाना आपके लिए अत्यंत महत्वपूर्ण है, इससे आपकी व्यक्तिगत सुरक्षा सुनिश्चित होती है और आपके डेटा, पैसे और मोबाइल की सुरक्षा का ध्यान रखा जाता है। इससे आपको अपराधों से बचाने में मदद मिलेगी और आपके जीवन के लिए महत्वपूर्ण है।

IX. सुरक्षित सोशल मीडिया और ऑनलाइन संचार :

a. गोपनीयता सेटिंग और ऑनलाइन प्रोफ़ाइल का प्रबंधन करना – आपकी व्यक्तिगत जानकारी आपकी होती है, इसलिए इसे सुरक्षित रखें। सोशल मीडिया पर अपनी प्रोफ़ाइल सेटिंग्स को समय–समय पर जांचें और सुनिश्चित करें कि केवल वह जानकारी शेयर की जाती है जिसे आप शेयर करना चाहते हैं।

b. **अत्याचारपूर्ण या परेशान करने वाले व्यवहार की पहचान और रिपोर्ट करना** – यदि आपको ऑनलाइन परेशान किया जाता है या कोई आपको अत्याचारित करता है, तो इसे जानें और इसकी रिपोर्ट करें। ऐसे व्यवहार को नजरअंदाज न करें, बल्कि इसे जगह–जगह रिपोर्ट करके सामाजिक मीडिया को सुरक्षित बनाएं।

c. **फ़ोटो और व्यक्तिगत जानकारी सुरक्षित रूप से साझा करना** – किसी भी व्यक्तिगत जानकारी या फ़ोटो को सोशल मीडिया पर साझा करने से पहले सोचें। इसे केवल उन लोगों के साथ साझा करें जिन्हें आप भरोसा करते हैं और जिनकी आपसे यह आवश्यकता होती है।

d. **ऑनलाइन मित्रों और संपर्कों की प्रामाणिकता की पुष्टि करना** – किसी भी व्यक्तिगत जानकारी या फ़ोटो को सोशल मीडिया पर साझा करने से पहले सोचें। इसे केवल उन लोगों के साथ साझा करें जिन्हें आप भरोसा करते हैं और जिनकी आपसे यह आवश्यकता होती है।

e. **व्यक्तिगत जानकारी को अधिक साझा करने से बचना** – आपकी व्यक्तिगत जानकारी का महत्व समझें और उसे बड़े पैमाने पर साझा न करें। ऑनलाइन जगत में आपकी सुरक्षा के लिए, व्यक्तिगत जानकारी को हमेशा सीमित रखें और उसे अनावश्यक स्थानों पर साझा न करें।

यह सरल तरीके आपको सुरक्षित रखेंगे और आपको साइबर दुनिया में सुरक्षित महसूस कराएंगे। इसके माध्यम से, आप और आपका गांव समझेंगे कि आपकी व्यक्तिगतता की रक्षा करना क्यों महत्वपूर्ण है और कैसे आप ऑनलाइन दुनिया में सुरक्षित रह सकते हैं।

x. **ऑनलाइन खरीदारी और बैंकिंग के लिए सुरक्षित तरीके :**

a. **ऑनलाइन विक्रेताओं और वेबसाइटों की वैधता की पुष्टि करना** – यह जानना ग्रामीण लोगों के लिए बहुत

महत्वपूर्ण है। आप इस तरीके से पता कर सकते हैं कि किसी विक्रेता या वेबसाइट की पुष्टि होती है या नहींरू जब आप किसी वेबसाइट पर खरीदारी करने के लिए जाते हैं, तो देखें कि वेबसाइट के ठीक ऊपर किसी छोटे तालिके का प्रतीक दिख रहा है जिसमें लॉक छाबी का चिन्ह होता है। इससे आपको पता चलेगा कि वेबसाइट सुरक्षित है और आप अपनी जानकारी सुरक्षित रख सकते हैं।

b. **सुरक्षित भुगतान विधियों और प्लेटफॉर्म का उपयोग करना** – गांव के लोग यह समझें कि सुरक्षित भुगतान विधियाँ और प्लेटफ़ॉर्म का उपयोग करने से वे खुद को सुरक्षित रख सकते हैं। आप एक सुरक्षित भुगतान प्लेटफॉर्म का उपयोग करके ऑनलाइन भुगतान कर सकते हैं, जैसे नेट बैंकिंग और डेबिट कार्ड। इससे आपकी वित्तीय जानकारी सुरक्षित रहेगी और आप चोरी के खतरे से बच सकेंगे।

c. **नकली ऑनलाइन खरीदारी वेबसाइटों और धोखाधड़ी से बचना** – यह सबसे महत्वपूर्ण है कि आप नकली ऑनलाइन खरीदारी वेबसाइटों और धोखाधड़ी से बचें। आपको ध्यान देना चाहिए कि आप केवल प्रमाणित और जाने माने वेबसाइटों से ही खरीदारी करें। अगर कोई वेबसाइट आपसे अत्याधिक छोटी कीमत पर वस्त्र या सामग्री बेचती है, तो संदेह करें। धोखाधड़ी से बचने के लिए हमेशा विश्वसनीय और प्रमाणित पेमेंट विकल्पों का उपयोग करें।

d. **ऑनलाइन लेन–देन के दौरान वित्तीय जानकारी की सुरक्षा करना** – आपको यह जानना ग्रामीण लोगों के लिए महत्वपूर्ण है कि आप अपनी वित्तीय जानकारी की सुरक्षा रखें जब आप ऑनलाइन लेन–देन करते हैं। अपनी खुद की जानकारी को सुरक्षित रखने के लिए, आपको एक सुरक्षित इंटरनेट कनेक्शन का उपयोग करना चाहिए। इसके अलावा, आपको अपना व्यक्तिगत जानकारी जैसे कि बैंक खाता नंबर और पासवर्ड को किसी के साथ नहीं साझा करना चाहिए।

गांव के लोगों को यह समझाना बहुत महत्वपूर्ण है कि ऑनलाइन खरीदारी और बैंकिंग के सुरक्षित तरीकों का उपयोग करके हम अपनी वित्तीय जानकारी की सुरक्षा बनाए रख सकते हैं और धोखाधड़ी से बच सकते हैं। इससे हमारा पैसा और हमारा बच्चों का भविष्य सुरक्षित रहेगा।

XI. अपनी और परिवार की साइबर खतरों से सुरक्षित रखने के तरीके :

a. **मजबूत और अद्वितीय पासवर्ड बनाना** – अपने ऑनलाइन खातों के लिए एक ताकतवर और अद्वितीय पासवर्ड चुनें। इसे याद रखने का प्रयास करें और किसी के साथ नहीं साझा करें।

b. **सॉफ़्टवेयर और एप्लिकेशनों को नियमित रूप से अपडेट करना** – अपने सभी सॉफ़्टवेयर, एप्लिकेशन और ऑपरेटिंग सिस्टम को नियमित रूप से अपडेट करें। इससे सुरक्षा नवीनतम सुधारों से लाभ मिलेगा और साइबर अभियांता के खिलाफ सुरक्षा बढ़ेगी।

c. **संदिग्ध लिंक पर क्लिक न करें और अज्ञात अटैचमेंट डाउनलोड न करें** – किसी भी संदिग्ध लिंक पर क्लिक न करें और नजरिये से अज्ञात अटैचमेंट डाउनलोड न करें। ऐसी गतिविधियाँ साइबर अपराधियों को आपके डिजिटल उपकरणों में प्रवेश करने का मौका देती हैं।

d. **ऑनलाइन पर्सनल जानकारी साझा करते समय सतर्क रहें** – जब आप ऑनलाइन पर्सनल जानकारी साझा करते हैं, तो सतर्क रहें। केवल विश्वसनीय और सुरक्षित वेबसाइटों पर ही अपनी जानकारी को साझा करें।

e. **ऑनलाइन अनुभवों के बारे में खुली बातचीत को प्रोत्साहित करें** – गांव के लोगों को यह समझाने के लिए प्रोत्साहित करें कि ऑनलाइन अनुभवों के बारे में खुलकर बातचीत करना महत्वपूर्ण है। यह साझा करना आपको और आपके परिवार को साइबर खतरों से बचाने का आसान तरीका है।

इन तरीकों के माध्यम से, आप और आपका परिवार साइबर खतरों से सुरक्षित रह सकते हैं। यह आपके डिजिटल जीवन की महत्वपूर्णता को समझाने के साथ–साथ आपको डिजिटल सुरक्षा की अवश्यकता को समझने में मदद करेगा।

XII. साइबर अपराधों के प्रतिक्रिया करना :

a. **साइबर अपराध का सामना करने पर लेने जाने वाले कदम** – जब हमारे गांव के लोगों को साइबर अपराध का सामना करना पड़ता है, तो हमें कुछ कदम उठाने होते हैं।

इसमें सबसे पहले यह समझना है कि कौनसे अपराध हो रहे हैं और कैसे हो रहे हैं। फिर हमें इन अपराधों के खिलाफ बचाव के लिए सावधान रहना चाहिए। जैसे, हमें सुरक्षित पासवर्ड उपयोग करना चाहिए और आवश्यकता होने पर संचार उपकरणों को अपडेट करना चाहिए।

b. **प्रासंगिक प्राधिकारियों को साइबर अपराध की रिपोर्ट करना** – यदि हमारे गांव में साइबर अपराध का सामना होता है, तो हमें इसकी रिपोर्ट संबंधित प्राधिकारियों को करनी चाहिए। इससे हम इन अपराधों के बारे में जागरूकता फैला सकते हैं और कानूनी कार्रवाई की आवश्यकता को जान सकते हैं।

c. **कानूनी कार्रवाई के लिए सबूत संरक्षित करना** – जब हमें साइबर अपराध का सामना होता है, तो हमें इसके सबूत संरक्षित करने की जरूरत होती है। इसके लिए हमें संदिग्ध गतिविधियों की स्क्रीनशॉट्स लेने चाहिए और इनकी प्रिंट आउट भी ले सकते हैं। इससे हमें कानूनी कार्रवाई करने में मदद मिल सकती है।

d. साइबर अपराध के पीड़ितों के लिए सहायता और संसाधनों की खोज करना – अगर हमारे गांव के लोगों को साइबर अपराध का शिकार हो जाते हैं, तो हमें उनकी मदद करनी चाहिए। हमें उन्हें जागरूक बनाना चाहिए कि उन्हें किसी भी संसाधन की आवश्यकता होती है, तो वे सहायता प्राप्त कर सकते हैं। हमें संगठनों और विशेषज्ञों के बारे में भी जानकारी देनी चाहिए जो साइबर अपराध के प्रति संवेदनशील हैं और उन्हें सहायता प्रदान कर सकते हैं।

इस तरह से हम गांव के लोगों को समझा सकते हैं कि साइबर अपराधों के खिलाफ कार्रवाई करना क्यों जरूरी है और उनके लिए कैसे महत्वपूर्ण है।

XII. सामुदायिक संज्ञान और प्रचार :

a. सामुदायिक में साइबर अपराध के बारे में जागरूकता को बढ़ावा देना – हमें साइबर अपराध के बारे में अपनी समुदाय में जागरूकता फैलानी होगी। यह अपराध हमारे डिजिटल सुरक्षा को खतरे में डाल सकते हैं।

b. **कार्यशालाओं और जागरूकता अभियानों का आयोजन करना** – हमें साइबर अपराध से बचने के तरीकों पर कार्यशालाओं और जागरूकता अभियानों का आयोजन करना होगा। इससे हम सभी लोग एक–दूसरे को सिखा सकेंगे और साथ मिलकर सुरक्षित रह सकेंगे।

c. **स्थानीय अधिकारियों, स्कूलों, सामुदायिक नेताओं, कानून प्रवर्तन संगठनों और संगठनों के साथ सहयोग करना** – हमें स्थानीय अधिकारियों, स्कूलों, सामुदायिक नेताओं, कानून प्रवर्तन संगठनों और संगठनों के साथ मिलकर मिलजुलकर काम करना होगा। यह हमारे गांव को सुरक्षित बनाने में मदद करेगा।

d. **व्यक्तियों को डिजिटल प्रचारक बनाना स्थानीय सहायता नेटवर्क और संसाधनों की स्थापना करना** – हमें अपने लोगों को डिजिटल प्रचारक बनाना होगा। इसके लिए हमें स्थानीय सहायता नेटवर्क और संसाधनों की स्थापना करनी होगी। इससे हम सभी को साइबर अपराधों से बचाने में मदद मिलेगी।

e. **गांवों के भीतर जागरूकता अभियान और कार्यशालाओं का आयोजन करना** – हमें अपने गांव के भीतर जागरूकता अभियान और कार्यशालाओं का आयोजन करना होगा। इससे हमारे गांव के लोग आसानी से समझ सकेंगे कि साइबर अपराधों से बचना क्यों जरूरी है और इसका महत्व क्या है।

इस तरीके से हम अपने गांव के लोगों को समझा सकेंगे कि साइबर अपराधों से बचना क्यों जरूरी है और हम सभी मिलकर एक सुरक्षित डिजिटल माहौल बना सकते हैं।

निष्कर्ष :

साइबर अपराध पर सर्वांगीण प्रशिक्षण मार्गप्रदर्शिका का उद्देश्य स्त्री एवं बच्चों और ग्रामीण गांवों में रहने वाले व्यक्तियों को उनको और उनके परिवारों को साइबर खतरों से सुरक्षित रखने के लिए आवश्यक ज्ञान और कौशल प्रदान करना है। अशोभनीय गतिविधियों के वृद्धि, यौन अपराधों, हिंसा और अनुचित गतिविधियों की प्रशंसा को संघटित करके, यह मार्गप्रदर्शिका समुदायों में एक सुरक्षित और जवाबदेह डिजिटल

संस्कृति को प्रचारित करने का प्रयास करती है। इस प्रशिक्षण के माध्यम से, प्रतिभागी साइबर अपराध, रोकथाम रणनीतियाँ और सहयोग की महत्वा की गहरी समझ प्राप्त करेंगे, अंततः सभी के लिए एक सुरक्षित डिजिटल वातावरण सृजित करेंगे।

इंटरनेट की लक्ष्मण रेखा–

कब हमारे द्वारा इंटरनेट पर की गई पोस्ट/मैसेज अपराध की श्रेणी में आ जाता है–

कई बार हमारे द्वारा इंटरनेट पर की गई पेास्ट या मैसेज अपराध की श्रेणी में आ जाता है और हमें पता भी नहीं चलता है। अभी हाल में ही कई ऐसे मामले सामने आये है, जहां किसी व्यक्ति द्वारा किये गये पोस्ट पर पुलिस ने प्राथमिकी दर्ज कर उसे जेल भेज दिया। ऐसे मामलों में उस व्यक्ति को पता भी नहीं होता है कि उसकी गलती क्या है। इंटनेट पर पोस्ट करते समय निम्न बातों का ध्यान रखना चाहिएः

1. किसी भी व्यक्ति/संस्था पर व्यक्तिगत टिप्पणी नहीं करनी चाहिए।

2. किसी धर्म अथवा राजनैतिक पोस्ट पर भड़काउ टिप्पणी नहीं करनी चाहिए।
3. बिना आश्वस्त हुए किसी भी मैसेज को शेयर नहीं करना चाहिए।
4. किसी दूसरे के नाम, फोटो तथा उसका पता का इस्तेमाल करते हुए सोशल मीडिया एकाउटं नहीं बनाना चाहिए।
5. किसी भी प्रकार का अश्लील सामग्री पोस्ट या शेयर नहीं करना चाहिए।

साईबर अपराध होने पर क्या करें :

किसी भी साईबर अपराध के शिकार या पीड़ित होने पर हमें अविलंब नजदीकी पुलिस स्टेशन से मदद लेनी चाहिए। पुलिस के पास जाने से पहले यथासंभव कोशिश करनी चाहिए कि इसकी शिकायत फोन द्वारा भारत सरकार के साईबर हेल्पलाईन नंबर–1930 पर शिकायत दर्ज कराये तथा ऑनलाईन शिकायत www.cybercrime.gov.in पर करें। बैंकिंग फ्रॉड होने पर बैंक को भी अविलंब सूचना देनी चाहिए।

पुलिस के पास निम्न कागजात के साथ जाना श्रेस्यकर होता है :

1. बैंकिंग फ्रॉड के मामलों में संदिग्ध लेनदेन का विवरणी बैंक से अपडेट कराकर पुलिस के पास जाना चाहिए।
2. सोशल मीडिया फ्रॉड होने पर स्क्रीन शॉट तथा URL का प्रिंट आउट लेकर पुलिस के पास जाना चाहिए।

कभी भी मोबाईल से स्क्रीन शॉन नहीं लेनी चाहिए।

साईबर अपराध से बचने के लिए क्या करें :

1. अपने सोशल मीडिया एकांउट/बैंक एकांउट में मजबूत पासवर्ड लगाये।
2. कंप्यूटर तथा मोबाईल में एंटी वायरस इंस्टॉल करें।
3. टू स्टेप वेरिफिकेशन का प्रयोग करें।

साईबर अपराध से बचने के लिए क्या न करें :

1. किसी भी अन्जान व्यक्ति से ऑनलाईन दोस्ती नहीं करें।
2. किसी भी व्यक्ति के साथ फोन पर अपना पासवर्ड/पीन या बैंकिंग डिटेल्स शेयर न करें।
3. अपनी व्यक्तिगत जानकारी सोशल मीडिया पर साझा न करें।
4. किसी भी अन्जान लिंक पर क्लिक न करें।
5. गूगल पर कस्टमर केयर का नंबर सर्च न करें, उसके आधिकारिक वेबसाईट पर जाकर नंबर सर्च करें।
6. अपने पासवर्ड के साथ यूजर आई0डी0 को भी गोपनीय रखें। किसी बाहरी के साथ अपना मोबाईल अथवा लैपटॉप शेयर न करें।

साइबरक्राइम रिपोर्ट कैसे करें?

- साइबरक्राइम की घटनाओं की रिपोर्ट करना एक आवश्यक कदम है जिससे पुलिस और अन्य संबंधित अधिकारियों को इन अपराधों का सामना करने में मददमिल सकती है। नीचे भारत में साइबरक्राइम की रिपोर्ट करने के चरण दिए गए हैं :
- **साइबरक्राइम विवरण संग्रहित करें :** सबसे पहले, आपको साइबरक्राइम के सभी विवरण संग्रहित करने की आवश्यकता होगी। यदि संभव हो, तोस्क्रीनशॉट लें, ईमेल्स सहेजें, और अन्य सबूत संग्रहित करें।
- **स्थानीय पुलिस स्थानक को सूचित करें :** अपने स्थानीय पुलिस स्थानक को अपराध के बारे में सूचित करें। आपको विवरण देने की आवश्यकता होगी औरयदि संभव हो, तो किसी भी सबूत की प्रतिलिपियाँ प्रस्तुत करें।
- **साइबर क्राइम रिपोर्टिंग पोर्टल पर जाएं :** भारत सरकार ने साइबरक्राइम की रिपोर्ट करने के लिए एक ऑनलाइन पोर्टल शुरू किया है (www.cybercrime.gov.in)। आप इस पोर्टल पर जाकर अपनी रिपोर्ट सबमिट कर सकते हैं।
- **रिपोर्ट सबमिट करें :** आपको अपनी व्यक्तिगत जानकारी, साइबरक्राइम की विवरण, और सबूत अपलोड करने की आवश्यकता होगी। फॉर्म को भरने केबाद, आपको रिपोर्ट सबमिट करनी होगी।
- रिपोर्ट की पुष्टि करेंरू आपको एक ईमेल याै डै के माध्यम से अपनी रिपोर्ट की पुष्टि की जाएगी। इसे सुरक्षित रखें, यह आपके केस का अनुसरण करने मेंमदद करेगा।
- **अपने केस का अनुसरण करें :** आप ऑनलाइन पोर्टल पर अपने केस का अनुसरण कर सकते हैं। आपको अपने केस की स्थिति के बारे में नियमित अपडेटप्राप्त होने चाहिए।

बिहार लोक प्रशासन
एवं
ग्रामीण विकास संस्थान

वाल्मी परिसर, फुलवारी शरीफ, पटना

टेली : – 91–612–2452585

फैक्स : – 91– 612–2452586

ईमेल : vidhimitra.bipard@gmail.com

वेबसाईट : www.bipard.bihar.gov.in