

संक्षिप्त रिपोर्ट (एग्जीक्यूटिव समरी)

स्टेटस ऑफ़ पुलिसिंग इन इंडिया रिपोर्ट 2026

साइबर अपराध—पीड़ितों के दृष्टिकोण और प्रणालीगत प्रतिक्रियाएँ

पिछले एक दशक में, साइबर अपराध भारत में रोज़मर्रा की ज़िंदगी का हिस्सा बन गया है। इसने नागरिकों के पैसे, उनका डेटा और ऑनलाइन सुरक्षा की भावना को हर तरह से प्रभावित किया है। यह किसी एक जगह या किसी एक प्रकार के पीड़ित तक सीमित नहीं है। फोन, बैंक खाता या सोशल मीडिया प्रोफ़ाइल रखने वाला हर व्यक्ति जोखिम में है। साइबर अपराध नेटवर्क पूरे भारत में फैल गए हैं। इन नेटवर्कों ने अधिकार-क्षेत्रों की हर सीमा को पार कर कई संस्थानों और समुदायों को प्रभावित किया और अंततः एक संगठित तंत्र के रूप में विकसित हो गए हैं।

इसी संदर्भ में, स्टेटस ऑफ़ पुलिसिंग इन इंडिया रिपोर्ट (एस.पी.आई.आर.) 2026: साइबरक्राइम—पीड़ितों के दृष्टिकोण और प्रणालीगत प्रतिक्रियाएँ—अपना ध्यान साइबर अपराध पर केंद्रित करती है। साइबर अपराध कैसे किया जाता है, इसका निशाना कौन बनता है, और नागरिक, पुलिस तथा बैंकिंग प्रणाली की इस पर किस प्रकार की प्रतिक्रिया होती है। पुलिस पर जनता के भरोसे और उसके साथ अनुभव पर एसपीआईआर श्रृंखला के फोकस को जारी रखते हुए, इस संस्करण में हमने साइबर अपराधियों के तौर-तरीकों, पीड़ितों के प्रत्यक्ष अनुभव, आम नागरिकों की डिजिटल आदतों और कमजोरियों, तथा शिकायतों से निपटने के लिए पुलिस और बैंकों की तैयारियों की पड़ताल की है।

एस.पी.आई.आर. का नवीनतम संस्करण कॉमन कॉज़ और लोकनीति-सी.एस.डी.एस. के संयुक्त रूप से संचालित अध्ययन का परिणाम है। यह अध्ययन भारत के 16 राज्यों में 8,306 से अधिक उत्तरदाताओं के बीच किए गए सर्वेक्षण पर आधारित है। इसका उद्देश्य भारत में साइबर अपराधों की तेजी से बदलती प्रकृति और उनसे निपटने के लिए बनाए गए तंत्रों की जांच करना है। अध्ययन का गुणात्मक (क्वालिटेटिव) घटक विस्तृत रूप से आमने-सामने किए गए साक्षात्कारों और एक फोकस समूह चर्चा (एफ.जी.डी.) पर आधारित है। इसमें क्षेत्र विशेषज्ञों, साइबर अपराध के पीड़ितों और उनकी निकटता से सहायता करने वाले 37 उत्तरदाताओं तथा साइबर अपराध के आरोप में आरोपित व्यक्तियों के परिजनों के साथ हुई बातचीत के निष्कर्ष प्रस्तुत किए गए हैं।

एस.पी.आई.आर. 2026 के प्रमुख निष्कर्ष नीचे प्रस्तुत किए गए हैं:-

गुणात्मक (क्वालिटेटिव) साक्षात्कारों से प्राप्त निष्कर्ष:

साइबर अपराध की संरचना: अपराध, रिपोर्टिंग में कमी और प्रभाव

- अपराध को अंजाम देने के लिए साइबर अपराधियों की निर्भरता “सोशल इंजीनियरिंग” पर बहुत अधिक होती है। वे संवेदनशील जानकारी या व्यक्तिगत उपकरणों तक पहुँच बनाने के लिए धोखे, हेरफेर, दबाव और धमकियों का उपयोग करते हैं।
- लीक हुए डेटा, म्यूल खातों और नकली सिम कार्डों की तैयार “किट” का कारोबार करते हुए संगठित नेटवर्क वित्तीय और गैर-वित्तीय दोनों तरह के साइबर अपराध चलाते हैं।
- सामाजिक कलंक के डर, अधिकारियों के प्रति अविश्वास, और शिकायतों को गंभीरता से न लिए जाने की भावना के कारण साइबर अपराध की व्यापक रूप से कम रिपोर्टिंग होती है। ऑनलाइन लैंगिक-आधारित हिंसा और बिना सहमति के छवियों (इमेज) के दुरुपयोग के अधिकांश मामले रिपोर्ट ही नहीं किए जाते हैं।
- पीड़ितों ने साइबर अपराध और उसके बाद चली शिकायत प्रक्रिया के कारण तनाव, आघात और अवसाद का वर्णन किया -- जिसमें एक गर्भपात, एक पीड़िता का अपना पेशा छोड़कर दूसरे देश में चले जाना, और एक अन्य का सेवानिवृत्ति के बाद अपनी जीवन भर की बचत खोने के बाद गंभीर अवसाद में चले जाना शामिल था।

संस्थागत प्रतिक्रियाएँ: एक कठिन और असमान राह

- साइबर अपराध के मामलों में आमतौर पर एफ़.आई.आर. दर्ज नहीं की जाती हैं। पुलिस से ऑनलाइन या व्यक्तिगत रूप से शिकायत करने वाले 15 पीड़ितों में से छः मामलों में एफ़.आई.आर. दर्ज की गई। इनमें से दो शिकायतें स्वतः एफ़.आई.आर. में बदल गई थी और कम से कम दो अन्य मामलों में पीड़ितों ने एफ़.आई.आर. दर्ज करवाने के लिए प्रभावशाली लोगों से संपर्क किया।
- वित्तीय साइबर अपराधों के पीड़ितों और विशेषज्ञों ने भारी बहुमत से महसूस किया कि बैंकों ने जवाबदेही लेने या पीड़ित को धन-वसूली की प्रक्रिया में सहायता करने से इनकार कर दिया। एक मामले को छोड़कर, वित्तीय धोखाधड़ी के पीड़ितों के साथ अन्य सभी साक्षात्कारों में, बैंकों ने कहा कि पीड़ितों ने धोखाधड़ी करने वाले के साथ “सहयोग” किया।
- वित्तीय साइबर अपराधों के पीड़ितों और विशेषज्ञों ने भारी बहुमत से महसूस किया कि बैंकों ने जवाबदेही लेने या पीड़ित को पैसे की रिकवरी की प्रक्रिया में सहायता करने से इनकार

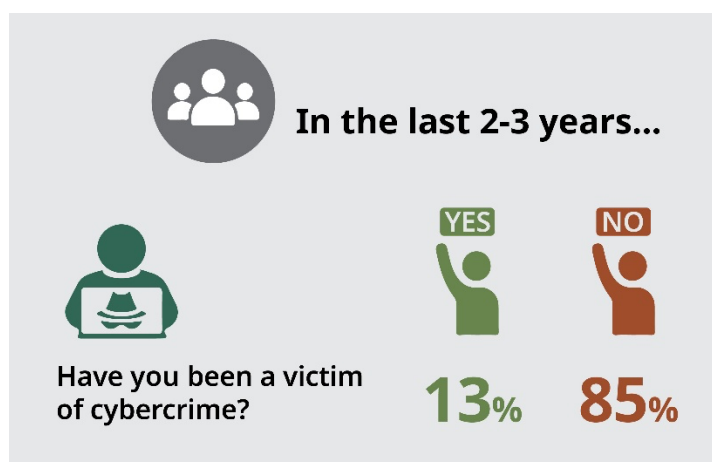
कर दिया। वित्तीय धोखाधड़ी के पीड़ितों में से एक को छोड़कर अन्य सभी साक्षात्कारों में यह बात निकल कर सामने आई कि बैंकों ने पीड़ितों पर धोखाधड़ी करने वाले के साथ “सहयोग” करने की बात कही।

- पुलिस के साथ अपने अनुभव को रेट करने वाले दस उत्तरदाताओं में, पुलिस को दी गई औसत रेटिंग पाँच में से 2.4 थी। बैंकों के साथ अपने अनुभव को रेट करने वाले छः पीड़ितों में, कुल रेटिंग पाँच में से एक, या खराब थी।

सर्वेक्षण निष्कर्ष: साइबर सुरक्षा, पीड़ितीकरण और साइबर अपराधों के लिए निवारण तंत्र

डिजिटल सुरक्षा के लिए खतरे और साइबर अपराध का शिकार होना:

- लगभग एक-तिहाई उत्तरदाताओं ने बताया कि उन्हें अक्सर फर्जी डिलीवरी संबंधी कॉल या अधिक रिटर्न वाले निवेश से जुड़ी स्कैम कॉल्स आए। लगभग एक-चौथाई उत्तरदाताओं ने बताया कि स्कैमर ने उन्हें अक्सर बैंक अधिकारी बनकर या अवैध गतिविधियों जांच करने वाला अफसर बनकर, तथा किसी मित्र के नाम पर किए जाने वाली कॉल की। आंकड़ों से पता चलता है कि ऑनलाइन भुगतान का अधिक उपयोग और धोखाधड़ीपूर्ण कॉलों का अधिक जोखिम का आपस में संबंध है।
- पिछले 2 से 3 वर्षों में 13 प्रतिशत उत्तरदाता साइबर अपराधों के शिकार हुए हैं। कम शिक्षित तथा युवा उत्तरदाताओं के साइबर अपराध का शिकार होने की संभावना अपेक्षाकृत अधिक है।

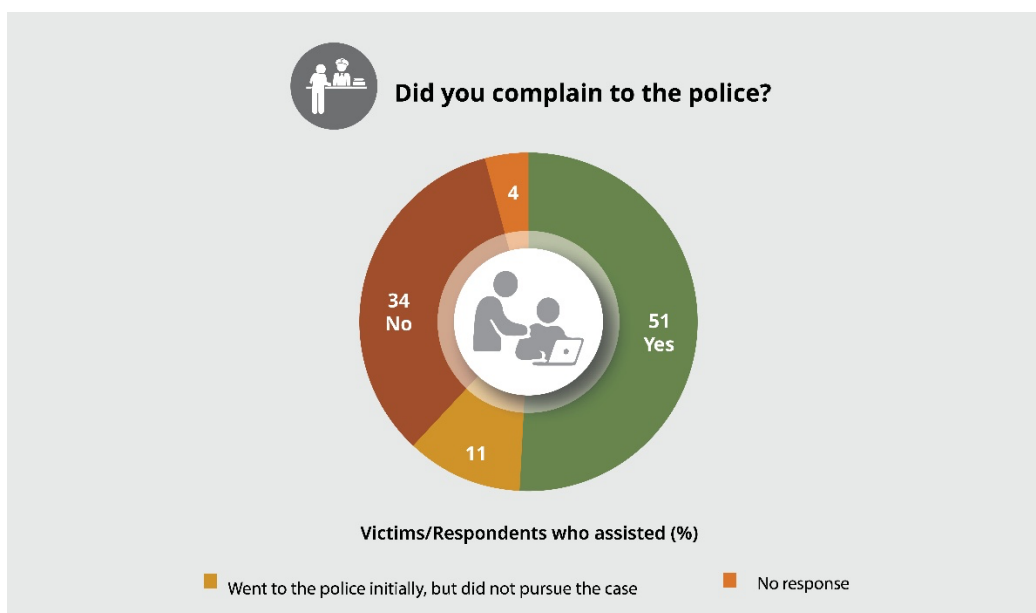


- रिपोर्ट किए गए सभी साइबर अपराधों में आधे से अधिक मामले डिजिटल वित्तीय धोखाधड़ी से संबंधित हैं। पीड़ितों में से 11 प्रतिशत ने व्यक्तिगत डेटा की चोरी होने, 7 प्रतिशत साइबर बुलिंग (ऑनलाइन उत्पीड़न) का शिकार होने, जबकि 4 प्रतिशत ने ऑनलाइन यौन उत्पीड़न के सामना करने की बात कही। उच्च वर्ग से आने वाले तथा अधिक शिक्षित उत्तरदाताओं के डिजिटल वित्तीय धोखाधड़ी का शिकार होने की संभावना अपेक्षाकृत अधिक पाई गई।

- डिजिटल वित्तीय धोखाधड़ी के शिकार लगभग एक-तिहाई पीड़ितों (31%) का मानना है कि उनकी व्यक्तिगत वित्तीय जानकारी बैंक के किसी अंदरूनी कर्मचारी (इनसाइडर) द्वारा लीक की गई थी। आर्थिक रूप से कमजोर पृष्ठभूमि वाले पीड़ितों में इस धारणा के पाए जाने की संभावना अपेक्षाकृत अधिक है।

पुलिस के साथ अनुभव

- साइबर अपराध की घटना के बाद लगभग आधे पीड़ितों (51%) ने पुलिस में शिकायत दर्ज कराई, जबकि 11 प्रतिशत पीड़ित प्रारंभ में पुलिस के पास गए, लेकिन बाद में मामले को आगे नहीं बढ़ाया।



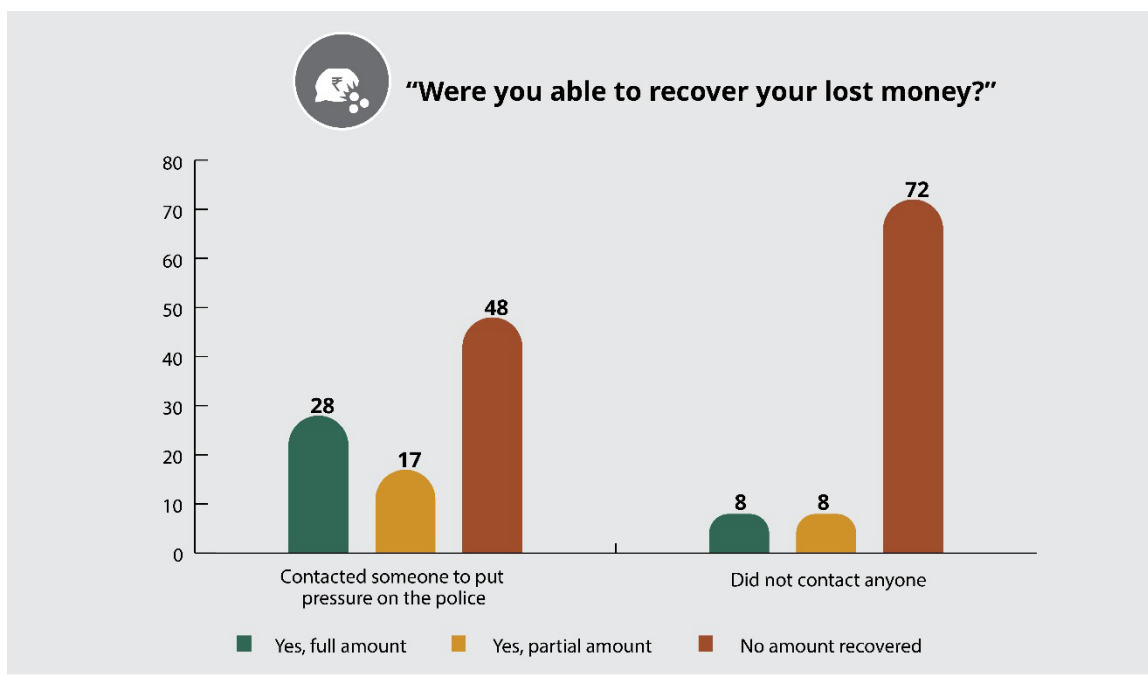
*Note: The figure includes responses from both the victims and those who assisted cybercrime victims.
 Question asked: Did you complain to the police?*

इस आकृति में पीड़ित और साइबरअपराध के पीड़ितों की सहायता करने वालों, दोनों के उत्तर शामिल हैं। पूछा गया प्रश्न: क्या आपने पुलिस में शिकायत की?

- पुलिस में शिकायत दर्ज कराने वाले पीड़ितों में लगभग एक-चौथाई को पाँच या उससे अधिक बार पुलिस थाने के चक्कर लगाने पड़े। शहरी क्षेत्रों के पीड़ितों की तुलना में ग्रामीण क्षेत्रों के पीड़ितों के पाँच या उससे अधिक बार पुलिस थाने जाने की संभावना अधिक पाई गई।
- पुलिस में शिकायत दर्ज कराने वाले पाँच में से दो पीड़ितों (42 प्रतिशत) ने शिकायत दर्ज कराने की प्रक्रिया को कठिन बताया। इनमें से 17 प्रतिशत ने इसे “बहुत कठिन” बताया, जबकि 25 प्रतिशत का कहना था कि यह प्रक्रिया “कुछ हद तक कठिन” थी।
- जिन उत्तरदाताओं ने पुलिस में अपनी शिकायत दर्ज कराई थी, उनमें से 27 प्रतिशत ने पुलिस को रिश्वत दी। आर्थिक रूप से कमजोर पीड़ितों के पुलिस को रिश्वत देने की संभावना संपन्न पीड़ितों की तुलना में लगभग चार गुना अधिक पाई गई। पुलिस को रिश्वत देने वाले पीड़ितों के साइबर अपराध में खोई

हुई पूरी राशि वापस प्राप्त करने की संभावना उन पीड़ितों की तुलना में तीन गुना अधिक थी, जिन्होंने रिश्तत नहीं दी थी।

- एक-तिहाई से अधिक पीड़ितों ने पुलिस से अपने मामले में सही कार्रवाई करवाने के लिए अपने परिचितों या जान-पहचान वाले लोगों की मदद ली। जिन पीड़ितों ने किसी परिचित के माध्यम से पुलिस से संपर्क किया, उनके साइबर अपराध में खोए हुए पूरे पैसे वापस मिलने की संभावना उन लोगों की तुलना में लगभग तीन गुना अधिक थी, जिन्होंने किसी की मदद नहीं ली।



नोट: शेष उत्तरदाताओं ने इन दोनों प्रश्नों में से किसी का भी उत्तर नहीं दिया। सभी आंकड़े प्रतिशत में हैं। तालिका में साइबर अपराध के पीड़ितों तथा पीड़ितों की सहायता करने वालों के उत्तर शामिल हैं।

बैंकों के साथ अनुभव

- डिजिटल वित्तीय धोखाधड़ी के हर दो पीड़ितों में से एक (52%) ने बैंक में अलग से शिकायत दर्ज कराई। वित्तीय धोखाधड़ी के लगभग दो-तिहाई पीड़ितों (63%) ने घटना के 24 घंटे के भीतर बैंक को इसकी सूचना दे दी थी।
- लगभग चार में से तीन पीड़ित (72%) अपनी गंवाई हुई राशि का कोई भी हिस्सा वापस नहीं पा सके।



Note: The rest did not respond. For more information on the index, refer to Appendix 2. The table includes responses from both the victims and those who assisted cybercrime victims of digital financial fraud.

Question asked: Were you able to recover your lost money?

नोट: शेष उत्तरदाताओं ने उत्तर नहीं दिया। सूचकांक पर अधिक जानकारी के लिए परिशिष्ट 2 देखें। इस आकृति में पीड़ित और डिजिटल वित्तीय फ्रॉड के साइबरअपराध के पीड़ितों की सहायता करने वालों, दोनों के उत्तर शामिल हैं। पूछा गया प्रश्न: क्या आप अपने गवांये गए पैसे की रिकवरी कर पाए?

- साइबर धोखाधड़ी के लगभग एक-चौथाई पीड़ित (22%) बैंक द्वारा धनराशि वापस दिलाने की भूमिका से 'बहुत असंतुष्ट' थे। वहीं, डिजिटल वित्तीय धोखाधड़ी के हर पाँच पीड़ितों में से एक (20%) अपने मामले में बैंक और पुलिस के बीच समन्वय से 'बहुत असंतुष्ट' था।

डिजिटल आदतें और साइबर सुरक्षा

- हर दो उत्तरदाताओं में से लगभग एक (49%) प्रतिदिन यूपीआई ऐप्स का उपयोग करते हैं। पुरुष, शहरी और उच्च वर्ग के उत्तरदाता अपने समकक्षों की तुलना में ऑनलाइन भुगतान के साधनों का अधिक उपयोग करते हैं।
- लगभग चार में से तीन उत्तरदाता (72%) प्रतिदिन सोशल मीडिया ऐप्स या वेबसाइटों का उपयोग करते हैं। कम आयु, उच्च आय वर्ग और शहरी क्षेत्रों के उत्तरदाताओं में सोशल मीडिया के नियमित उपयोग की संभावना अन्य समूहों की तुलना में अधिक पाई गई।
- जो लोग नियमित रूप से यूपीआई का उपयोग करते हैं, उनके साइबर अपराध का शिकार होने की संभावना उन लोगों की तुलना में अधिक होती है, जो इसका नियमित उपयोग नहीं करते हैं।

यूपीआई उपयोग और साइबर अपराध का शिकार होने की संभावना	
	पिछले 2-3 वर्षों में क्या आप साइबर अपराध का शिकार हुए हैं?

यूपीआई का उपयोग	हाँ (%)	नहीं (%)
कई बार	16	81
कभी-कभी	12	85
कभी नहीं	7	89

नोट: सभी आंकड़े प्रतिशत में हैं। शेष उत्तरदाताओं ने उत्तर नहीं दिया। 'कभी नहीं' और 'मैं ऑनलाइन भुगतान नहीं करता/करती' की श्रेणियों को मिलाकर 'कभी नहीं' श्रेणी बनाई गई है।

- प्रत्येक पाँच में से एक व्यक्ति (20%) ने बताया कि वे यूपीआई ऐप्स के माध्यम से लेन-देन करते समय टू-स्टेप वेरिफिकेशन का उपयोग नहीं करते हैं। युवा, अधिक शिक्षित, शहरी तथा आर्थिक रूप से संपन्न उत्तरदाताओं में अपने समकक्षों की तुलना में यूपीआई ऐप्स पर टू-स्टेप वेरिफिकेशन का उपयोग करने की संभावना अधिक पाई गई।
- पाँच में से एक उत्तरदाता (21%) ने बताया कि वे हमेशा सुरक्षित साइबर व्यवहारों का पालन करते हैं, जैसे सार्वजनिक वाई-फाई के उपयोग से बचना, ऐप की अनुमतियों (Permissions) की जांच करना, तथा वेबसाइट या ऐप की प्रामाणिकता की पुष्टि करना। वहीं 21 प्रतिशत उत्तरदाताओं ने कहा कि वे ऐसी सावधानियों का कभी पालन नहीं करते। युवा, अधिक शिक्षित तथा शहरी क्षेत्रों के उत्तरदाताओं में अपने समकक्षों की तुलना में इन सुरक्षित साइबर व्यवहारों का पालन करने की संभावना अधिक पाई गई।

संस्थानों पर भरोसा और आगे की राह

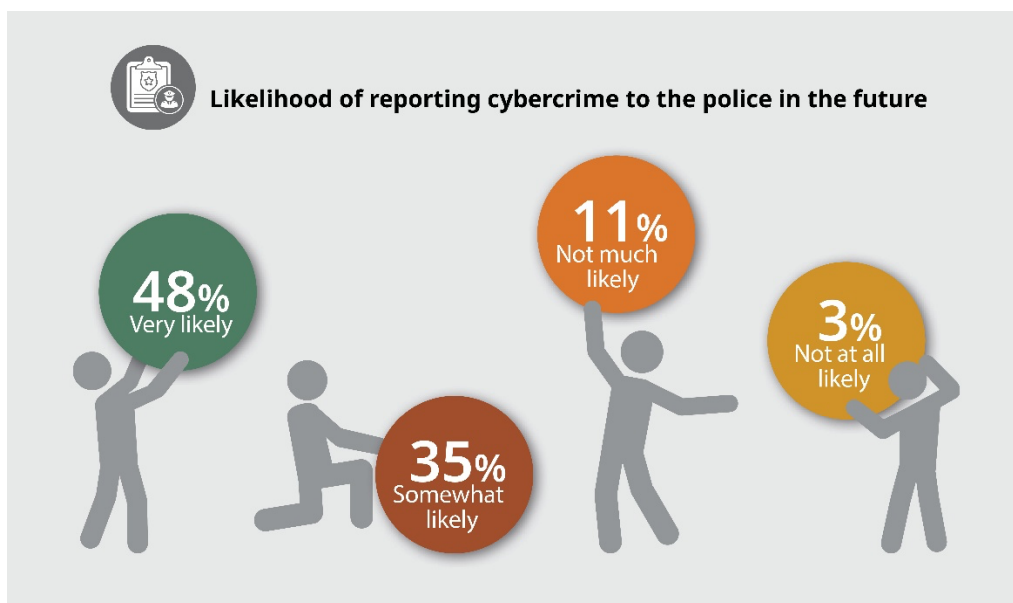
- लगभग चार में से तीन लोगों का मानना है कि वित्तीय साइबर अपराधों से निपटने के लिए पुलिस के पास आवश्यक क्षमता और संसाधन मौजूद हैं। इनमें से 29 प्रतिशत का मानना है कि पुलिस "पूरी तरह सक्षम" है, जबकि 44 प्रतिशत लोगों का कहना है कि पुलिस "कुछ हद तक सक्षम" है।
- साइबर अपराध के पीड़ितों में यह विश्वास अपेक्षाकृत कम पाया गया कि पुलिस साइबर अपराध के मामलों से प्रभावी ढंग से निपटने में पूरी तरह सक्षम है। हालांकि, पीड़ितों में वे लोग जिन्होंने पुलिस में शिकायत दर्ज कराई थी, अन्य पीड़ितों की तुलना में थोड़ा अधिक मानते हैं कि पुलिस साइबर अपराधों से निपटने के लिए पर्याप्त रूप से सक्षम है।

	साइबर अपराधों से निपटने के लिए पुलिस...			
	पूरी तरह सक्षम	कुछ हद तक सक्षम	बहुत अधिक सक्षम नहीं	बिल्कुल भी सक्षम नहीं
कुल मिलाकर	29	44	17	7
पीड़ित/सहायता करने वाले उत्तरदाता	23	44	21	10
गैर-पीड़ित	31	44	15	6

नोट: सभी आंकड़े प्रतिशत में हैं। प्रस्तुत आंकड़ों में केवल उन उत्तरदाताओं को शामिल किया गया है जिन्होंने स्वयं को साइबर अपराध का पीड़ित बताया था, तथा वे उत्तरदाता जिन्होंने साइबर अपराध के पीड़ितों की सहायता की थी।

पूछा गया प्रश्न: आपकी राय में वित्तीय साइबर अपराधों से निपटने के लिए पुलिस कितनी सक्षम है?--पूरी तरह सक्षम, कुछ हद तक सक्षम, बहुत अधिक सक्षम नहीं, या बिल्कुल भी सक्षम नहीं।

- बैंक और पुलिस की साइबर अपराधों से निपटने के पर्याप्त रूप से प्रशिक्षित होने के सवाल पर साइबर अपराध के पीड़ितों में सकारात्मक धारणा अपेक्षाकृत कम पाई गई। गैर-पीड़ितों की तुलना में पीड़ितों के यह मानने की संभावना कम थी कि बैंक और पुलिस ऐसे मामलों से प्रभावी ढंग से निपटने के लिए अच्छी तरह प्रशिक्षित हैं। हालांकि, पीड़ितों में वे लोग जिन्होंने अलग से पुलिस या बैंक में शिकायत दर्ज कराई थी, अन्य पीड़ितों की तुलना में थोड़ा अधिक मानते हैं कि ये संस्थान साइबर अपराधों से निपटने के लिए पर्याप्त रूप से प्रशिक्षित हैं।
- लगभग आधे उत्तरदाताओं (48%) ने कहा कि यदि वे भविष्य में साइबर अपराध का शिकार होने पर पुलिस को सूचना देने की उनकी संभावना बहुत अधिक है। हालांकि, साइबर अपराध के पीड़ितों में यह कहने की संभावना अपेक्षाकृत कम पाई गई कि भविष्य में ऐसी घटना होने पर वे पुलिस में शिकायत दर्ज कराएंगे।



Note: The rest did not respond. All figures are in percentages.

Question asked: If you are a victim of a case of cybercrime in the future, how likely are you to report the case to the police - very likely, somewhat likely, not much likely, or not at all likely?

नोट: शेष उत्तरदाताओं ने उत्तर नहीं दिया। सभी आंकड़े प्रतिशत में हैं। पूछा गया प्रश्न: यदि भविष्य में आप साइबर अपराध का शिकार होते हैं, तो इसकी शिकायत पुलिस को करने की कितनी संभावना है?--बहुत अधिक संभावना, कुछ हद तक संभावना, कम संभावना, या बिल्कुल भी संभावना नहीं।



रिपोर्ट की कॉपी डाउनलोड करने के लिए
कृपया क्यूआर कोड स्कैन करें या नीचे दिये
गए लिंक पर क्लिक करें।

https://commoncause.in/pdf/SPIR_2026.pdf