eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

डिजिटल युग में बैंकिंग क्षेत्र की प्रतिबंधक प्रणाली साइबर सुरक्षाः चुनौती एवं समाधान

डॉ0 सोना धनगर[1], श्री सुनील मिश्रा[2]
[1]अतिथि शिक्षक विधि विभाग बी0जी0आर0 परिसर, हे0न0ब0ग0 विश्वविद्यालय (केन्द्रीय विश्वविद्यालय) श्रीनगर गढ़वाल, उत्तराखण्ड
[2]अधिवक्ता, बार एसोसिएशन श्रीनगर. पौड़ी गढ़वाल, उत्तराखण्ड

Received: 26 Dec 2025 Accepted & Reviewed: 28 Dec 2025, Published: 31 December 2025

Abstract

बैंकों की सुरक्षा प्रणाली के लिए साइबर सुरक्षा एक महत्वपूर्ण भाग है, क्योंकि बैंकों में ग्राहकों का न सिर्फ पैसा वर्न उनकी संवेदनशील निजी एवं वित्तीय जानकारी भी होती है। यही कारण है कि ग्राहकों की इनकी निजी जानकारी होना ही साइबर आक्रमणों का केन्द्र बना रहता है और यही हमले और इनके होने की आशंका बैंकों को सुदृढ़ सुरक्षा प्रणाली को बनाने को मजबूर करती है। ग्राहकों का भरोसा इसी सुरक्षा प्रणाली की वजह से आकर्षित होता है, जिसको दाव पे लगाके कोई भी बैंक जोखिम नहीं उठाना चाहेगा। सुरक्षा प्रणाली में हुई एक छोटी सी चूक बैंक की वर्षों से बनी साख को सेकिंडों में खाक में मिला सकती है और जाहिर है कि कोई भी बैंक वित्तीय नुकसान को अपनी किसी भूल के कारण क्यों ही वहन करना स्वीकार करेगा। वैश्वीकरण के वर्तमान दौर में, इंटरनेट बैंकिंग या आनलाइन बैंकिंग ने 21वीं सदी के आधुनिक बैंकिंग युग में क्रांति सी ला दी है। मनुष्य सुचनाओं, विचारों और ज्ञान के आदान–प्रदान के लिए विभिन्न उपायों को विकसित करता रहता है, जो उनके लिए अत्याधिक महत्व रखते हैं। इलेक्ट्रॉनिक बैंकिंग तकनीक में हुई प्रगति ने बैंकिंग कार्य को बेहद आसान बना दिया है। बैंकिंग कार्य ऑनलाइन बैंकिंग और एंड्रॉइड मोबाइल फ़ोन के माध्यम से शीर्घता से सम्पन्न हो रहे हैं अब बैंकिंग लेन–देन एक क्लिक मात्र की दूरी पर है।

वर्ष 2016 की नोटबन्दी और यूपीआई की लॉन्चिंग ने भारत की बैंकिंग को हमेशा के लिए बदल दिया है। जो कार्य पहले पासबुक अपडेट कराने के लिए लाइन में लगकर होता था, वह अब एक फत् स्कैन पर हो जाता है। भारतीय राष्ट्रीय भुगतान निगम के डेटा के अनुसार अप्रैल 2026 में यूपनआई ने 18 अरब ट्रांजैक्शन का आंकडा पार कर लिया है। परन्तु साइबरस्पेस में सूचना प्रौद्योयोगिकी के बढ़ते दुरूपयो से राष्ट्रीय और अन्तर्राष्ट्रीय स्तर पर साइबर अपराध बढ़ रहे हैं। जोखिम और उससे जुडी समस्याओं की संख्या दिन प्रति दिन बढ़ती ही जा रही है। RBI Report on Trend and Progress of Banking in India 2024–25 बताती है कि डिजिटल पेमेंट फ्रॉड की राशि पिछले 3 वर्ष में 5 गुना बढ़ी है। इस आधार पर कहा जा सकता है कि ऑनलाइन और मोबाइल बैंकिंग अभी भी सुरक्षित नहीं होता है। इस लेख का उद्देश्य साइबर हमलों की समीक्षा करना है और बैकिंग से जुडे साइबर अपराधों और हैकर्स द्वारा अपनाई जाने वाली नई तरकीबों और तरीकों पर केंद्रित है। यह अध्ययन पूरी तरह से सहायक डेटा पर आधारित है। इस अध्ययन के निष्कर्ष भारत में आईटी के बढ़ते उपयोग और ऑनलाइन बैंकिंग से जुडे साइबद अपराधों को उजागर करते हैं। इस लेख के माध्यम से ऑनलाइन बैंकिंग में अपराधों की रोकथाम और सुरक्षित उपयोग के लिए कुछ सुझाव भी दिए गये हैं।

मुख्य शब्द– सूचना प्रौद्योयोगिकी, साइबर अपराध, साइबर हमला, मोबाइल बैंकिंग, ऑनलाइन बैंकिंग, राष्ट्रीय अपराध रिकार्डिंग कार्यालय, हैकिंग।

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

Introduction

भारत में बैंकिंग का इतिहास सदियों पुराना है, किन्तु पिछले दो दशकों में इसका चेहरा पूरी तरह बदला सा गया है। एक समय था जब बैंक का मतलब लंबी लाइन, लेन–देन हेतु फ़ॉर्म भरना, पासबुक अपडेट एवं चेक क्लियर होने के लिए 3 दिन का इंतजार। 1969 में बैंकों के राष्ट्रीयकरण के बाद ब्रांच बैंकिंग का विस्तार हुआ। गांव–कस्बों तक बैंक पहुंचे। लोगों का पैसा सुरक्षित हुआ और बचत की आदत बढ़ी। किन्तु इस सिस्टम की सीमा थी। खाता खोलने से लेकर लोन लेने तक प्रत्येक कार्य को कागज पर किया जाता था। बैंक के खुलने का समय प्रातः 11 से 2 बजे तक, शनिवार को आधा दिन और रविवार को अवकाश का प्रावधान था। आपातकाल में पैसा निकालना मानो नामुमकिन था। कैश किंग हुआ करता था और ट्रांजैक्शन में समय व श्रम दोनों लगता था। 1970 का दशक साइबर सुरक्षा की वास्तविक शुरूआत और आवश्यकता का दौर था, यही वह समय था जब एडवांस्ड रिसर्च प्रोजेक्ट्स एजेंसी नेटवर्क की पहल की गयी थी और इसी के माध्यम से नेटवर्क और डिवाइस को बाहरी खतरों से सुरक्षित किया जाता है। 1980 में बैंकों में रिकॉर्ड रखने और सेवाओं के लिए पर्सनल कम्प्यूटर का इस्तेमाल शुरू हुआ और 1982–85 के दौर मे भारतीय बैंकिंग में धीरे–धीरे कम्प्यूटरीकरण को बढ़ावा मिला। सुरक्षा के इसी आयाम को सुदृढ़ बनाने के दृष्टिकोण से कंपनियां अपनी गोपनीयता और अपने कर्मचारियों की निजी जानकारियों को सुरक्षित रखने कें लिए कंपनी में विशेषज्ञों की नियुक्ति करती हैं। ताकि इन विशेषज्ञों के कोशल से साइबर हमलों से बचा जा सके। तब से वर्तमान तक बैंकिंग क्षेत्र ने ग्राहकों के विस्वास को कायम रखने के उद्देश्य से सुरक्षा के अनेक तरीके अपनाए हैं। 1990 के दशक में निजी और विदेशी बैंकों ने कौर बैंकिंग कनेक्टिविटी शुरू की, जिसके बाद सरकारी बैंकों ने भी इसका इस्तेमाल शुरू किया।

बैंकिंग का डिजिटल ट्रांसफॉर्मेशन– इंटरनेट के आने से बैंकिंग क्षेत्र पूरी तरह से बदल गया, खासकर सुरक्षा के मामले में, क्योंकि अब हमारी धनराशि बस एक क्लिक में हमारे हाथ में है। उपयोगकर्ता विभिन्न तरीकों से अपने पैसे का प्रबंधन कर सकते हैं। इलेक्ट्रॉनिक बैंकिंग डिलीवरी चौनलों के माध्यम से बैंकिंग उत्पादों और सेवाओं का प्रावधान है। इस बैंकिंग प्रणाली के माध्यम से ग्राहक को इंटरनेट के जरिए से धनराशि के लेन–देन के लिए एक और विकल्प मिला इलेक्ट्रॉनिक बैंकिंग। 1990 के दशक में बैंक में कम्प्यूटर आना बड़ी बात थी, वर्ष 2010 तक कोर बैंकिंग साल्यूशन यानी सी0बी0एस0 आया। किन्तु असली गैम चेन्जर 2016 के बाद बना जब बैंक ने अपने सिस्टम के दरवाजे फिनटेक के लिए खोले। Open Banking API के जरिए आज फोन–पे, गूगल–पे, क्रेड जैसी सैकड़ों ऐप सीधे आपके बैंक अकाउंट से जुड़ी हैं। इसका फायदा इनोवेशन में हो सकता है और नुकसान वर्तमान में साइबर अटैक सरफेस 10 गुना हो गया है। पहले हैकर को बैंक का मेन सर्वर तोड़ना पड़ता था। अब किसी कमजोर फिनटेक पार्टनर का UPI हैक करके भी वो बैंक तक पहुंच सकता है। 2023 का iMobile Pay केस इसी का उदाहरण है।

आने वाले कुछ वर्षों में, कृत्रिम बुद्धिमत्ता और मशीन लर्निंग वित्तीय सेवा उद्योग में साइबर सुरक्षा के मुख्य चालक बने रहेंगे। हम बाजार में पहले से ही व्यवस्थित कुछ अधिक उन्नत सुरक्षा उत्पादों में इसे देखना शुरू कर चुके हैं, जैसे कि अच्छे बाट बनाम बुरे लोग। जोखिम और प्रतिफल के मामले में स्वचालन एक और महत्वपूर्ण कारक है, क्योंकि बैंक और क्रेडिट युनियन हर उस चीज को स्वचालित करने की कोशिश कर रहे हैं जिसे वे कर सकते हैं। हम और भी अधिक लो–कोड और नो–कोड प्लेटफ़ॉर्म देखेंगे जिनका उद्देश्य मानवीय त्रुटि को कम करते हुए वित्तीय संस्थानों की दक्षता में सुधार करना है। ऑनलाइन

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

बैंकिंग हर किसी के लिए फिजिकल और पेपरलेस बैंकिंग को मुफ्त बनाती है और इसके साथ–साथ वह ऑनलाइन बैंकिंग बैंकों की परिचालन लागत को भी कम करती है, क्योंकि इससे 4,444 ग्राहकों से जुड़ी लागतें कम होती हैं और उनकी शाखाओं का नेटवर्क भी छोटा हो जाता है। अब ऑनलाइन बैंकिंग का रोजाना इस्तेमाल लोंगों के लिए दैनिक लेन–देन का एक आम चलन बन गया है। ऐसे कार्यक्रम, योजनाएँ और नीतियाँ जो साइबर सुरक्षा में इस कौशल की कमी को दूर करती है। साइबर सुरक्षा में पीढ़ी के अंतर को पाटना और इस क्षेत्र में अधिक विविधता लाना आज की एक और महत्वपूर्ण प्राथमिकता है। सइबर सुरक्षा का अर्थ है ऐसी तकनीकों और कार्यप्रणालियों का समूह, जिन्हें नेटवर्क, डिवाइस आदि को किसी भी हमले, क्षति यो अनधिकृत पहुँच से बचाने के लिए डिजाइन किया गया है। साइबर सुरक्षा, तकनीकों, प्रक्रियाओं और नियंत्रणों का उपयोग करके सिस्टम, नेटवर्क, प्रोग्राम, डिवाइस और डेटा को साइबर हमलों से बचाने का एक अभ्यास है। इसका उद्देश्य साइबर हमलों को कम करना और सिस्टम, नेटवर्क तथा तकनीकों के अनधिकृत दुरूपयोग से सुरक्षा प्रदान करना है।

इस लेख का मुख्य विषय ऑनलाइन बैंकिंग में साइबर सिक्योरिटी के लाभ और चुनौतियों का मूल्यांकन करना है, यह ऑनलाइन बैंकिंग सेवाओं के सामने आने वाली चुनौतियों का विश्लेषण करता है, और साइबर अपराध को नियंत्रित करने तथा उससे बचाव के लिए निवारक उपायों व सुरक्षा संबंधी सुझावों की पेशकश करता है। क्या आपको नहीं लगता कि हमारे ऑनलाइन फंड्स भी भरोसेमंद सुरक्षा के हकदार हैं? यहीं पर साइबर सुरक्षा काम आती है। साइबर सुरक्षा कंप्यूटर, सेवाओं, मोबाइल उपकरणों, इलेक्ट्रॉनिक प्रणालियों, नेटवर्क और डेटा को दुर्भावनापूर्ण हमलों से बचाने का एक तरीका है। इसे सूचना प्रौद्योगिकी सुरक्षा या इलेक्ट्रॉनिक सूचना सुरक्षा के रूप में भी जाना जाता है। इस शब्द का उपयोग विभिन्न संदर्भों में किया जाता है, व्यापार से लेकर मोबाइल कंप्यूटिंग तक, और इसे कुछ सामान्य श्रेणियों में विभाजित किया जा सकता है। नेटवर्क सुरक्षा कंप्यूटर नेटवर्क को घुसपैठियों से बचाने का एक तरीका है, चाहे वे लक्षित हमलावर हों या अवसरवादी मैलवेयर। एप्लिकेशन सुरक्षा सॉफ्टवेयर और उपकरणों को खतरों से बचाने पर केंद्रित है। खतरे में पड़े एप्लिकेशन उस डेटा तक पहुंच प्रदान कर सकते हैं जिसे वे बचाने के लिए डिज़ाइन किए गए हैं। सफल सुरक्षा डिज़ाइन चरण से ही शुरू होती है, किसी प्रोग्राम या उपकरण को तैनात किए जाने से बहुत पहले। सूचना सुरक्षा भंडारण और प्रसारण के दौरान डेटा की अखंडता और गोपनीयता की रक्षा करती है। परिचालन सुरक्षा में डेटा संपत्तियों को संभालने और सुरक्षित करने की प्रक्रियाएं और समाधान शामिल हैं।

नेटवर्क तक पहुंचने पर उपयोगकर्ताओं के पास मौजूद अनुमतियों को प्रबंधित करने की प्रक्रियाएं, और डेटा को कैसे और कहाँ संग्रहीत या साझा किया जा सकता है, इस श्रेणी में आते हैं। आपदा रिकवरी और व्यावसायिक निरंतरता यह परिभाषित करती है कि संगठन साइबर सुरक्षा घटनाओं या अन्य घटनाओं पर कैसे प्रतिक्रिया देते हैं, जिनके परिणामस्वरूप परिचालन या डेटा का नुकसान होता है। एक आपदा रिकवरी नीति यह परिभाषित करती है कि कोई संगठन परिचालन और जानकारी को कैसे पुनर्प्राप्त करता है ताकि किसी घटना से पहले की तरह ही परिचालन क्षमता पर वापस आ सके। व्यावसायिक निरंतरता एक ऐसी योजना है जिस पर संगठन तब निर्भर रहते हैं जब वे कुछ संसाधनों के बिना काम करने की कोशिश कर रहे होते हैं। अंतिम–उपयोगकर्ता प्रशिक्षण साइबर सुरक्षा के सबसे अप्रत्याशित तत्व, यानी लोगों पर केंद्रित है। कोई भी व्यक्ति जो सुरक्षा सिफारिशों का पालन नहीं करता है, वह गलती से किसी सुरक्षित

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

प्रणाली में वायरस डाल सकता है। उपयोगकर्ताओं को संदिग्ध ईमेल अटैचमेंट हटाने और अपरिचित नेट्ठ ड्राइव को कनेक्ट करना बंद करने के बारे में शिक्षित करना किसी भी संगठन की सुरक्षा के लिए अत्यंत महत्वपूर्ण है।

ऑनलाइन बैंकिंग के फ़ायदे–

1) सुविधा– ऑनलाइन बैंकिंग अपने ग्राहकों को ज़बरदस्त सुविधा देती है। हमारे स्मार्टफ़ोन और कंप्यूटर हमेशा उपलब्ध रहते हैं और आपके खाते तक 24/7 पहुँच देते हैं। ऑनलाइन बैंकिंग से आप अपने घर या ऑफ़िस में आराम से बैठकर, बस एक बटन दबाकर अपने खाते तक पहुँच सकते हैं और पेमेंट कर सकते हैं। ऑनलाइन बैंकिंग के साथ–साथ, खाते को रिन्यू कराने, नए चेक लेने और ऐसी ही दूसरी लेन–देन के लिए नॉन–ट्रेडिंग फ़ंड का भी इस्तेमाल किया जा सकता है।

2) सुरक्षा– जब ग्राहक ऑनलाइन बैंकिंग का इस्तेमाल करते हैं, तो वित्तीय संस्थानों के लिए सुरक्षा सबसे बड़ी प्राथमिकता होती है। बैंक खाते की सुरक्षा को बहुत गंभीरता से लेते हैं और आपके खाते को सुरक्षित रखने के लिए बहुत सारा समय और पैसा लगाते हैं। ऑनलाइन खाते की सुरक्षा। कई मोबाइल बैंकिंग ऐप्लिकेशन अब लॉगिन के लिए एन्क्रिप्टेड बायोमेट्रिक प्रमाणीकरण स्वीकार करते हैं। जब कोई जुड़ा हुआ बैंक लॉगिन के लिए अतिरिक्त सत्यापन का अनुरोध करता है, तो बैंक कुछ खास तरह के जोखिमों से अपने–आप सुरक्षा भी दे सकता है। जैसे कि किसी अनजान डिवाइस से इस्तेमाल किए जाने पर।

3) ऑनलाइन इनवॉइस पेमेंट– आसान खाता लॉगिन और कुशल ऑनलाइन बिलिंग के साथ। ऑटोमैटिक बिल पेमेंट सुविधा के लिए आपको बस एक बार कुछ जानकारी डालनी होती है। बैंक हर पेमेंट का स्टेटमेंट मेल या मैसेज से भेजता है।

4) मोबिलिटी– पिछले कुछ सालों में ऑनलाइन बैंकिंग ने मोबाइल इंटरनेट बैंकिंग के रूप में एक और कदम आगे बढ़ाया है और अब यह असीमित मोबिलिटी के दायरे को भी कवर करती है।

5) रेमिटेंस (पैसे भेजना)– ऑनलाइन बैंकिंग एक खाते से दूसरे खाते में पैसे ट्रांसफर करने की प्रक्रिया को तेज़ कर देती है, जिससे समय और पैसे की बचत होती है और यह ज़्यादा सुविधाजनक बन जाता है। ट्रांज़ैक्शन देखने के लिए, ऑनलाइन बैंकिंग आपको कहीं से भी अपने खाते की हिस्ट्री और ट्रांज़ैक्शन देखने की सुविधा देती है। ऐसा इसलिए है क्योंकि यह सबसे तेज़ तरीका है।

6) लागत में कमी– ऑनलाइन बैंकिंग की फ़ीस कम होती है, या हो सकता है कि कोई फ़ीस ही न लगे।

साइबर सुरक्षा हेतु मुख्य आधार

1. गोपनीयता (Privacy)
2. अखंडता (Integrity)
3. उपलब्धता (Availability)
4. प्रामाणिकता (Authenticity)
5. अस्वीकार न कर पाना (Non&Repudiation)

अब हम आपको इन पाँचों आधारों को एक–एक करके समझने में मदद करेंगे।

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

1) गोपनीयता– गोपनीयता साइबर सुरक्षा के सबसे महत्वपूर्ण आधारों में से एक है। यह सुनिश्चित करता है कि आपका डेटा किसी के सामने (किसी भी अनाधिकृत समूह, संस्था या डिवाइस के सामने) ज़ाहिर न हो। जब डेटा सुरक्षा की बात आती है, तो गोपनीयता एक बहुत ही महत्वपूर्ण हिस्सा होती है। जब डेटा एक जगह से दूसरी जगह भेजा जाता है, तो उसे एन्क्रिप्ट (गुप्त कोड में बदलना) कर दिया जाता है। ईमेल में दी गई जानकारी को केवल उसे भेजने वाला और उसे पाने वाला ही समझ सकता है। किसी भी तीसरी पार्टी (थर्ड पार्टी) के लिए आपके डेटा को चुराना बहुत मुश्किल होता है। जी हाँ। जब आप अपने दोस्तों के साथ चौट करते हैं, तो आपके मैसेज एन्क्रिप्टेड होते हैं। कोई भी तीसरी पार्टी आपके मैसेज नहीं पढ़ सकती। केवल आप और आपके दोस्त ही उन मैसेज को सही–सही समझ सकते हैं। अब ज़रा सोचिए कि अगर कोई और व्यक्ति आपके ये सारे मैसेज पढ़ ले, तो क्या होगा? क्या यह एक बहुत बड़ी मुसीबत नहीं होगी? आपने अपनी निजी जानकारी शेयर की थी, और अब वह जानकारी किसी तीसरी पार्टी के पास भी पहुँच गई है। अब वह जानकारी तीसरी पार्टी के पास उपलब्ध है। हो सकता है कि आपको कई अलग–अलग तरह की सेवाओं के लिए न्योता (invitation) भी मिलने लगें। इसलिए, गोपनीयता या जानकारी को गुप्त रखना बहुत ज़रूरी है। जब तक आपकी बातचीत निजी रहती है, तब तक आपकी निजी जानकारी भी सुरक्षित रहती है। आप बिना किसी चिंता के, जो चाहें वह कर सकते हैं। इसलिए, गोपनीयता का मतलब है, डेटा तक पहुँच को नियंत्रित करने के लिए पासवर्ड, एन्क्रिप्शन और बायोमेट्रिक स्कैनिंग जैसी तकनीकों का इस्तेमाल करना।

2) अखंडता – किसी को भेजा गया मैसेज हमेशा अपने मूल रूप में ही स्टोर होता है। मैसेज को रास्ते में बदला नहीं जाना चाहिए। डेटा को तीसरे पक्षों द्वारा छेड़छाड़ से सुरक्षित रखें। आपके डेटा को उसके मूल रूप में रखने के लिए एक प्रभावी सुरक्षा प्रणाली बनाई गई है। तीसरे पक्ष आपकी सहमति के बिना आपकी जानकारी नहीं बदल सकते। यदि आपका डेटा आपकी अनुमति के बिना बदल दिया गया है, तो इसका सीधा सा मतलब है कि किसी ने आपके डेटा के साथ छेड़छाड़ की है। ईमानदार मॉडल। मान लीजिए आप Instagram इस्तेमाल कर रहे हैं और अपने दोस्तों के साथ चौट कर रहे हैं। किसी ने आपको बीच में टोका, और जिस व्यक्ति को आपने मैसेज भेजा था, उसने मैसेज मिलने से पहले ही उसे एडिट कर दिया। इससे आपके और जिस व्यक्ति से आप बात कर रहे हैं, उसके बीच बहुत सारी समस्याएं पैदा हो सकती हैं। हाँ। मैंने अपना क्रेडिट कार्ड इस्तेमाल किया, और वह अचानक काम करना बंद कर गया। जब मैंने अधिकारियों से संपर्क किया, तो उन्होंने मुझे बताया कि जानकारी बदल गई थी। आप इस पर कैसे प्रतिक्रिया देंगे? आप सकारात्मक रूप से प्रतिक्रिया दे सकते हैं। इसलिए, ऐसी घटनाओं को रोकने के लिए डेटा अखंडता (Data Integrity) ज़रूरी है। डेटा को उसके मूल फ़ॉर्मेट में रखा जाता है, और तीसरे पक्षों द्वारा किसी भी तरह के बदलाव की अनुमति नहीं होती है।

3) उपलब्धता – पहुँच का मतलब है कि आपका डेटा कोई भी व्यक्ति, जिसके पास उसे एक्सेस करने की अनुमति है, किसी भी समय आसानी से एक्सेस कर सकता है। किसी भी तरह से, यह आपके सिस्टम को पूरी तरह से चालू रखेगा। अपनी सुविधा के अनुसार अपना डेटा एक्सेस करें। संसाधनों की उपलब्धता उन्हें उपलब्ध जानकारी तक आसानी से पहुँचने में मदद करती है। उपलब्धता के लिए संसाधनों की ज़रूरत होती है ताकि स्थिरता बनी रहे और समय पर अपडेट और रखरखाव के ज़रिए डेटा तक लगातार पहुँच बनी रहे। उदाहरण– बहुत से लोग ऑनलाइन बैंकिंग का इस्तेमाल करते हैं। मान लीजिए कि सभी लेन–देन

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

ऑनलाइन बैंकिंग के ज़रिए किए जाते हैं। आप अपने लेन–देन का इतिहास और खाते का बैलेंस देखना चाहते हैं। अब, मान लीजिए कि आपका बैंक दिन के कुछ खास समय पर ही इस जानकारी तक पहुँच देता है। उस समय आप जो महसूस करेंगे, उसे शब्दों में बयान नहीं किया जा सकता। इसलिए, इससे बचने के लिए, कंपनी ज़रूरत पड़ने पर (यदि अधिकृत हो) जानकारी तक पहुँच देने की कोशिश करती है। यह याद रखना ज़रूरी है कि आग लगने और बिजली गुल होने जैसी घटनाएँ हो सकती हैं, जिससे आपका डेटा हैकर्स के लिए असुरक्षित हो सकता है।

4) प्रामाणिकता– प्रमाणीकरण डेटा को हैकर्स से बचाता है और यूज़र्स से डेटा तक पहुँचने का प्रमाण देने की माँग करता है। डेटा तक तभी पहुँचें जब आपके पास उस तक पहुँचने का अधिकार हो। जानकारी और लिंक्स के स्रोतों की जाँच करना महत्वपूर्ण है। प्रमाणीकरण नियंत्रणों में पासवर्ड, बायोमेट्रिक्स और कई अन्य तरीके शामिल हैं। आइए प्रामाणिकता को बेहतर ढंग से समझने के लिए एक उदाहरण देखें। हाँ, बहुत से लोग Instagram का उपयोग करते हैं। अपने यूज़रनेम और पासवर्ड के साथ अपने खाते में लॉग इन करें। अब, मान लीजिए कि Instagram किसी को बिना पासवर्ड या यूज़रनेम माँगे आपके खाते तक पहुँचने की अनुमति दे देता है। और इस व्यक्ति ने आपका डेटा चुरा लिया, जिसमें आपकी फ़ोटो और अन्य चीज़ें शामिल हैं। यह सब होने के बाद आपको कैसा लगेगा? क्या यह अच्छा लगेगा? उनमें से कुछ तो आत्महत्या करने के बारे में भी सोच सकते हैं। लेकिन प्रामाणिकता, जो साइबर सुरक्षा का एक स्तंभ है, इन सभी चीज़ों का ध्यान रखती है। अनधिकृत लोगों और उपकरणों को आपकी जानकारी तक पहुँचने से रोकें। यह तभी संभव है जब लोगों के पास आपके डेटा तक पहुँच हो।

5) विश्वसनीयता– नॉन–रेप्यूडिएशन यह सुनिश्चित करने में एक और महत्वपूर्ण कारक है कि डेटा केवल भेजने वाले को ही भेजा जाए। यह सुनिश्चित करता है कि संदेश प्राप्त करने वाला भी भेजने वाले की पहचान सत्यापित कर सके। आप सूचना सुरक्षा प्रणाली द्वारा प्रदान किए गए लॉग्स को खोलकर भेजने वाले और प्राप्त करने वाले की पहचान सत्यापित कर सकते हैं। कोई भी तीसरा पक्ष आपकी जानकारी के भेजने और प्राप्त करने को नियंत्रित नहीं कर सकता; केवल दो लोग ही भेजे गए संदेश को संशोधित कर सकते हैं, एक–दूसरे के लिए। यह उदाहरण हमें नेटवर्क सुरक्षा के दूसरे तत्वकृनॉन–रेप्यूडिएशन, को बेहतर ढंग से समझने में मदद करता है। आप मुझे इसलिए टेक्स्ट करते हैं क्योंकि आप अपने दोस्तों के साथ चौट करना चाहते हैं। और संदेश आपके दोस्तों के अलावा किसी और को भेज दिया जाता है। अब आप इस स्तंभ के महत्व की कल्पना कर सकते हैं। इस तरह, आपका संदेश केवल आपके दोस्तों को ही भेजा जाएगा, किसी और को नहीं।

साइबर सुरक्षा के प्रकार–

1) ऐप सुरक्षा–

• आप अपने फ़ोन पर जिन ज़्यादातर ऐप्स का इस्तेमाल करते हैं, वे सुरक्षित होते हैं और Google Play Store के नियमों और कानूनों के हिसाब से काम करते हैं।

• यूज़र 1.85 मिलियन अलग–अलग ऐप्स डाउनलोड कर सकते हैं। सिर्फ़ इसलिए कि दूसरे विकल्प मौजूद हैं, सभी ऐप्स सुरक्षित नहीं होते।

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

• कई ऐप्स सुरक्षित होने का दिखावा करते हैं, लेकिन हमसे सारी जानकारी लेने के बाद, ऐप का यूज़र पैसों के बदले तीसरे पक्षों के साथ जानकारी शेयर करता है, और फिर ऐप काम करना बंद कर देता है।

अचानक साइबर हमला– ऐप को Google Chrome के अलावा किसी भरोसेमंद प्लेटफ़ॉर्म से ही इंस्टॉल करना चाहिए। साइबर सुरक्षा के लिए 11 बेहतरीन सुझाव–

•अपने डेटा का बैकअप लें–अपने डिवाइस पर मौजूद डेटा को किसी दूसरी, अलग जगह पर कॉपी करके उसका बैकअप लेना, सबसे ज़रूरी कामों में से एक है जो आप कर सकते हैं। अगर आप पर कोई साइबर हमला होता है, तो हो सकता है कि आप अपने PC, लैपटॉप, फ़ोन या किसी भी दूसरे डिवाइस को एक्सेस या इस्तेमाल न कर पाएं। लेकिन अगर आपने अपने डेटा का बैकअप लिया हुआ है, तो आपके डिवाइस के साथ कुछ भी हो जाए, आपका कुछ भी नहीं खोएगा।

•अपने ऐप्स को अप–टू–डेट रखें–जब आपको पता चले कि आपके डिवाइस या किसी ऐप का अपडेट आया है, तो उसे नज़रअंदाज़ न करें; उसे जितनी जल्दी हो सके इंस्टॉल कर लें। आपको अपने फ़ीचर्स अपडेट करते रहना चाहिए। ये अपडेट अक्सर सुरक्षा से जुड़ी कमियों को ठीक करने के लिए भी होते हैं। आपके डिवाइस या ऐप में ऐसी कमियां हो सकती हैं, जिन्हें साइबर हमलावर ढूंढकर आपके सिस्टम तक पहुँचने के लिए इस्तेमाल कर सकते हैं। अगर आपके डिवाइस को अब कोई अपडेट नहीं मिल रहा है, तो आपको एक नए मॉडल में अपग्रेड करने के बारे में सोचना चाहिए।

•अपने डिवाइस के सॉफ़्टवेयर और ऐप्स को अपडेट करें।

•अपने सिस्टम की सेटिंग्स को अपने–आप अपडेट होने (automatically update) पर सेट कर दें, ताकि आपको चिंता न करनी पड़े। – अपने डिवाइस से उन सभी ऐप्स को हटा दें, जिनका इस्तेमाल आप अब और नहीं करते हैं।

2) एक अनोखा पासवर्ड चुनें– आजकल हम सभी के इतने ज़्यादा ऑनलाइन अकाउंट हैं कि उन सभी के लिए ज़रूरी पासवर्ड को याद रखना मुश्किल हो गया है। इस समस्या से निपटने के लिए, हममें से कई लोग अपने सभी अकाउंट के लिए एक ही पासवर्ड का इस्तेमाल करते हैं, या फिर बस दो–तीन अलग–अलग पासवर्ड ही बार–बार इस्तेमाल करते रहते हैं। इसमें दिक्कत यह है कि अगर किसी साइबर हमलावर को आपके किसी एक अकाउंट का पासवर्ड मिल जाता है, तो अक्सर उसे आपके कई दूसरे अकाउंट का एक्सेस भी मिल जाता है।

आप जितने भी ऑनलाइन अकाउंट बनाते हैं, उन सभी के लिए अलग–अलग पासवर्ड का इस्तेमाल करें।

- अपने पासवर्ड स्टोर और मैनेज करने के लिए पासवर्ड मैनेजर इस्तेमाल करके देखें।
- पासवर्ड मैनेजर ही एकमात्र ऐसा अकाउंट है जिसके लॉगिन डिटेल्स आपको याद रखने की ज़रूरत है।
- पासवर्ड बनाने के लिए छोटे पासवर्ड इस्तेमाल करें या पासवर्ड की जगह कुछ रैंडम शब्द जोड़ें।

3) टू–फैक्टर ऑथेंटिकेशन चालू करें– टू–फैक्टर ऑथेंटिकेशन एक ऐसा तरीका है जिससे आप अपने ऑनलाइन ट्रांज़ैक्शन को हैक होने से बचाने में मदद कर सकते हैं। आप अपने डिवाइस, जैसे कि फ़ोन पर एक कोड भेजने या जेनरेट करने का विकल्प भी चुन सकते हैं, जिसका इस्तेमाल आप हर बार लॉगिन

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

करते समय अपनी पहचान वेरिफ़ाई करने के लिए कर सकते हैं। इस तरह, अगर किसी को आपके अकाउंट का पासवर्ड मिल भी जाता है, लेकिन अगर उनके पास कोड पाने के लिए आपका फ़ोन नहीं है, तो आपका अकाउंट सुरक्षित रहेगा।

• ईमेल और सोशल नेटवर्किंग अकाउंट जैसे ज़रूरी अकाउंट के लिए टू–फैक्टर ऑथेंटिकेशन चालू करें।

• अगर एक से ज़्यादा विकल्प उपलब्ध हैं, तो SMS के अलावा कोई दूसरा विकल्प चुनें, क्योंकि SMS कम सुरक्षित होता है।

• दूसरे फ़ैक्टर के तौर पर SMS का इस्तेमाल करना, टू–फैक्टर ऑथेंटिकेशन का बिल्कुल भी इस्तेमाल न करने से कहीं ज़्यादा सुरक्षित है।

• टू–फैक्टर ऑथेंटिकेशन (2FA) आपके ऑनलाइन अकाउंट को हैक होने से बचाने का एक और तरीका है।

• आप फ़ोन जैसे किसी डिवाइस पर कोड भेजने या जेनरेट करने का विकल्प चुन सकते हैं, जिसका इस्तेमाल आप हर बार लॉगिन करते समय अपनी पहचान वेरिफ़ाई करने के लिए कर सकते हैं।

• इसलिए, अगर किसी को आपके अकाउंट का पासवर्ड मिल भी जाता है, तो भी वे आपके अकाउंट में तब तक लॉगिन नहीं कर पाएँगे, जब तक उनके पास कोड पाने के लिए आपका मोबाइल फ़ोन न हो।

4) मोबाइल सुरक्षा से जुड़ी बातें–

1) सबसे पहले, आपको इस फ़ोन पर सभी सुरक्षा पैच (security patches) इंस्टॉल करने होंगे।

2) आपको अपने फ़ोन के इन–बिल्ट ऐप का इस्तेमाल करके सभी पेमेंट ऐप्स को लॉक कर देना चाहिए, और अपने फ़ोन का पासवर्ड अपने परिवार के बाहर किसी के साथ कभी भी शेयर नहीं करना चाहिए।

• आप इनमें से कोई एक तरीका अपना सकते हैं–

• एक एक्सटर्नल हार्ड ड्राइव लें और ऑफ़लाइन या कोल्ड बैकअप करें, या – Dropbox जैसी क्लाउड–बेस्ड सर्विस के लिए साइन अप करें और क्लाउड बैकअप करें।

• अपने डेटा का नियमित रूप से (जैसे, हर हफ़्ते) बैकअप लेते रहें।

5) अपने अकाउंट रिकवरी सवालों के जवाब देने में क्रिएटिव बनें– जब आप कोई नया ऑनलाइन अकाउंट बनाते हैं, तो अक्सर आपसे अपने अकाउंट को सुरक्षित रखने और उसे रिकवर करने के लिए एक पासवर्ड सेट करने को कहा जाता है। इसका इस्तेमाल आम तौर पर तब किसी यूज़र की पहचान करने के लिए किया जाता है, जब वे अपना पासवर्ड भूल जाते हैं और उन्हें किसी हिंट की ज़रूरत होती है। ये सवाल अक्सर ऐसी चीज़ों पर आधारित होते हैं जिन्हें याद रखना आसान हो, जैसे आपके पहले पालतू जानवर का नाम या आप किस स्कूल में पढ़े थे। बदकिस्मती से, हमलावरों के लिए इन चीज़ों का पता लगाना आसान होता है, और वे आपकी जानकारी के बिना आपके अकाउंट तक पहुँचने के लिए इनका इस्तेमाल कर सकते हैं।

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

• जब आपसे अकाउंट रिकवरी से जुड़े सवाल पूछे जाएँ, तो जवाब देने में क्रिएटिव बनें। उदाहरण के लिए, आप किस स्कूल में पढ़े थे, इस बारे में सच बताने के बजाय आप "IPC" लिख सकते हैं।

6) फ्री हॉटस्पॉट Wi-Fi पर ज़रूरी लेन–देन करने से बचें– जब आप हॉटस्पॉट या फ्री Wi-Fi (जैसे, किसी कॉफ़ी शॉप में) का इस्तेमाल कर रहे हों, तो यह ध्यान रखना एक अच्छा विचार है कि आप ऑनलाइन क्या कर रहे हैं, क्योंकि ये नेटवर्क अक्सर सुरक्षित नहीं होते हैं। अगर आपका नेटवर्क सुरक्षित नहीं है, तो कोई भी उस तक पहुँच सकता है और आपका डेटा हासिल कर सकता है। इस बात का भी खतरा रहता है कि लोग आपके कंधे के ऊपर से झाँककर आपकी लॉगिन डिटेल्स देख लें। इसलिए, जहाँ आप खबरें या मौसम का हाल तो देख सकते हैं, वहीं ज़्यादा संवेदनशील लेन–देन करने से बचने की कोशिश करें। अगर मुमकिन हो, तो किसी और के डिवाइस के बजाय अपने खुद के डिवाइस का इस्तेमाल करें।

7) एंटीवायरस सॉफ़्टवेयर इंस्टॉल करें और नियमित रूप से वायरस के लिए स्कैन करें– एंटीवायरस सॉफ़्टवेयर आपके कंप्यूटर सिस्टम से मैलवेयर (वायरस) का पता लगाने और उन्हें हटाने में आपकी मदद कर सकता है। यदि आप Microsoft Windows 7 या उसके बाद का वर्शन चला रहे हैं, तो इसमें Windows Defender नाम का एक मुफ़्त एंटीवायरस पहले से आता है। अन्यथा, किसी जानी–मानी और भरोसेमंद कंपनी से कोई असली एंटीवायरस खरीदें। आपकी स्थानीय कंप्यूटर सर्विस कंपनी आपको सलाह दे सकती है कि आपके लिए कौन सा तरीका सबसे अच्छा है। ऑनलाइन मिलने वाला मुफ़्त एंटीवायरस सॉफ़्टवेयर डाउनलोड न करें। क्योंकि ऐसे कई प्रोग्राम जिनका विज्ञापन मुफ़्त के तौर पर किया जाता है, वे असल में नकली होते हैं। मैलवेयर या एडवेयर का पता लगाने और उन्हें हटाने के बजाय, वे खुद आपके कंप्यूटर पर डाउनलोड हो सकते हैं।

समाधान

• अपने कंप्यूटर पर एक एंटीवायरस प्रोग्राम इंस्टॉल करें। यदि आपको पक्का नहीं है कि आप यह खुद कर सकते हैं या नहीं, तो कोई कंप्यूटर सर्विस कंपनी आपके लिए यह काम कर सकती है।

- इसे नियमित रूप से (जैसे हर हफ़्ते) चलाएँ और पाए गए वायरस को हटाएँ।
- अगली बार जब भी आपको कोई वायरस मिले, तो अपने IT प्रोफ़ेशनल को उसकी जानकारी दें।

8) सोशल नेटवर्क पर ध्यान दें– क्या आप जानते हैं कि जो जानकारी आप अपनी Facebook प्रोफ़ाइल, Twitter फ़ीड, या प्देजंहतंउ अकाउंट पर पोस्ट करते हैं, उसका इस्तेमाल आपकी पहचान चुराने या आपके ऑनलाइन अकाउंट को हैक करने के लिए किया जा सकता है? हमें ऑनलाइन चीज़ें शेयर करने की इतनी आदत हो गई है कि हम इस बारे में सोचते भी नहीं हैं। हर किसी को आपके पालतू जानवर का नाम, स्कूल, नौकरी, और यहाँ तक कि आप छुट्टियों पर कब जा रहे हैं, यह सब पता होता है। दुर्भाग्य से, यह जानकारी न केवल आपके दोस्तों और परिवार को यह बताती है कि आप क्या कर रहे हैं, बल्कि ऐसी जानकारी भी देती है जिसका इस्तेमाल साइबर अपराधी आपके डेटा तक पहुँचने या आपकी पहचान चुराने के लिए कर सकते हैं।

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

• अपने सोशल मीडिया अकाउंट की प्राइवेसी पक्की करें। अपनी पूरी जानकारी सिर्फ़ अपने दोस्तों और परिवार वालों को ही दिखाई देने लायक सेट करें। अपने सोशल मीडिया अकाउंट पर बहुत ज़्यादा निजी जानकारी पोस्ट न करें।

• पासवर्ड के बारे में दी गई सलाह याद रखें। अगर आप थ्रमइववा पर अपने कुत्ते की कोई फ़ोटो शेयर करते हैं, तो पक्का करें कि आप अपने कुत्ते का नाम अपने पासवर्ड के तौर पर इस्तेमाल न करें।

9) ऑनलाइन दी जाने वाली निजी जानकारी को सीमित रखें– स्कैम और फ़िशिंग ईमेल अक्सर असली कंपनियों, जैसे बैंकों, का रूप धरकर आपको निजी या वित्तीय जानकारी देने के लिए धोखा देते हैं। यह जानना इसलिए ज़रूरी है ताकि आप समझ सकें कि कौन से अनुरोध असली हैं और कौन से नहीं। जब तक आपको यह न पता हो कि जानकारी कौन माँग रहा है और क्यों, तब तक ऑनलाइन निजी जानकारी न दें।

• निजी जानकारी देने से पहले रुकें और पुष्टि करें। पता करें कि जिन कंपनियों के साथ आप लेन–देन करते हैं, वे आपसे कैसे संपर्क करेंगी और वे आपसे कौन सी जानकारी माँगेंगी। उदाहरण के लिए, आपका बैंक आपको कभी भी ऑनलाइन बैंकिंग का लिंक ईमेल नहीं करेगा और न ही आपसे लॉग इन करने के लिए कहेगा।

• अगर आपको पक्का नहीं पता कि आपसे जानकारी देने के लिए क्यों कहा जा रहा है, तो सीधे उस कंपनी को फ़ोन करके पता करें कि जानकारी की ज़रूरत क्यों है। कंपनियों के लिए यह ज़रूरी है कि वे सिर्फ़ वही जानकारी माँगें जो कानून के हिसाब से ज़रूरी हो।

• अगर आपको निजी या वित्तीय जानकारी के लिए कोई ऑनलाइन अनुरोध मिलता है जिसके बारे में आपको पक्का नहीं पता, तो जानकारी देने से पहले उसकी पृष्ठभूमि की जाँच करें। उदाहरण के लिए, अगर आपकी बीमा कंपनी ऑनलाइन जानकारी माँग रही है, तो पहले फ़ोन करें या, अगर हो सके, तो अपने स्थानीय ऑफ़िस जाकर जानकारी के बारे में पूछें।

10) बैंक स्टेटमेंट चेक करें– अपने बैंक स्टेटमेंट में किसी भी संदिग्ध गतिविधि, जैसे कि अचानक की गई खरीदारी या खातों के बीच हुए ट्रांसफर, की जाँच करें। यदि आपको कोई भी असामान्य गतिविधि दिखाई देती है, तो तुरंत अपने बैंक से संपर्क करें। यदि आप देखते हैं कि कोई आपके बैंक खाते में पैसे ट्रांसफर कर रहा है या आपके क्रेडिट कार्ड से अचानक कोई पेमेंट कर रहा है, तो यह इस बात का पहला संकेत हो सकता है कि किसी ने आपके खाते या क्रेडिट कार्ड की जानकारी तक पहुँच बना ली है।

• अपने बैंक खातों और क्रेडिट कार्ड पर नज़र रखें, और हमेशा अपने स्टेटमेंट चेक करते रहें।

• जैसे ही आपको कोई संदिग्ध पेमेंट या निकासी दिखाई दे, तुरंत अपने बैंक को कॉल करें।

11) क्रेडिट चेक करवाएँ– अपने बैंक खाते पर नज़र रखने से आपको यह पता लगाने में मदद मिल सकती है कि क्या कोई और आपके खाते तक पहुँच बना रहा है। क्रेडिट चेक से आपको यह पता चल सकता है कि क्या कोई और आपकी निजी जानकारी का इस्तेमाल करके लोन ले रहा है, या किसी बड़ी खरीदारी (जैसे कार) के लिए लोन ले रहा है। अक्सर, आपको इस गतिविधि के बारे में सबसे पहले तब पता चलता

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

है जब आपका लोन अस्वीकार हो जाता है या जब पैसे वसूलने वाले लोग आपके दरवाज़े पर आ जाते हैं। अपनी क्रेडिट हिस्ट्री पर नज़र रखने से आपको किसी भी अनाधिकृत गतिविधि के बारे में पहले से ही चेतावनी मिल सकती है।

- हर साल अपना क्रेडिट चेक करवाएँ।

- यदि आपको कुछ भी संदिग्ध दिखाई दे, तो तुरंत कार्रवाई करें। अपने बैंक या फाइनेंस कंपनी को कॉल करके उन्हें स्थिति के बारे में सूचित करें और पूछें कि वे आपकी किस प्रकार मदद कर सकते हैं।

साइबर सुरक्षा समाधान – साइबर हमलों से खुद को सुरक्षित रखें।

1) अपने सॉफ्टवेयर और ऑपरेटिंग सिस्टम को अपडेट रखें। इसका मतलब है कि आप लेटेस्ट सुरक्षा अपडेट्स का लाभ उठा सकते हैं।

2) सुरक्षा समाधान के लिए Kaspersky Total Security जैसे एंटीवायरस सॉफ्टवेयर का उपयोग करें; यह खतरों का पता लगाता है, उन्हें हटाता है और सुरक्षा के सर्वोत्तम स्तर के लिए आपके सॉफ्टवेयर को अपडेटेड रखता है।

3) एक मजबूत पासवर्ड का उपयोग करें ताकि यह सुनिश्चित हो सके कि आपके पासवर्ड का अनुमान लगाना कठिन हो।

4) अज्ञात भेजने वालों से आए ईमेल अटैचमेंट्स को न खोलें, क्योंकि उनमें मैलवेयर हो सकता है।

5) सार्वजनिक स्थानों पर असुरक्षित WI-FI नेटवर्क्स का उपयोग करने से बचें। एक असुरक्षित नेटवर्क मैन–इन–द–मिडिल हमलों के प्रति संवेदनशील होता है।

निष्कर्ष– डिजिटल इंडिया के इस दौर में बैंकिंग की परिभाषा पूरी तरह बदल चुकी है। जो काम कभी ब्रांच की लंबी लाइनों और पासबुक एंट्री से होता था, वह आज मोबाइल स्क्रीन पर एक टैप से पूरा हो जाता है। UPI, इंटरनेट बैंकिंग, मोबाइल वॉलेट और अब CBDC ने आम आदमी को 24•7 वित्तीय आजादी दी है। पर इसी आजादी के साथ एक नई चुनौती भी खड़ी हो गई है, साइबर सुरक्षा। बैंक अब सिर्फ पैसे के रखवाले नहीं, बल्कि करोड़ों लोगों के डेटा के संरक्षक भी हैं। और यह डेटा, साइबर अपराधियों के लिए सोने की खान से कम नहीं। RBI की रिपोर्ट्स बताती हैं कि डिजिटल पेमेंट फ्रॉड के मामले हर साल बढ़ रहे हैं। फिशिंग, स्मिशिंग, नकली बैंकिंग ऐप, अकाउंट टेकओवर और रैंसमवेयर जैसे हमले अब बड़े बैंकों से लेकर छोटे को–ऑपरेटिव बैंकों तक को निशाना बना रहे हैं। अपराधियों का तरीका भी अब पहले से ज्यादा शातिर हो गया है। वे बैंक के नाम से हूबहू मिलती–जुलती वेबसाइट बनाते हैं, कस्टमर केयर बनकर फोन करते हैं और डर या लालच दिखाकर OTP मांग लेते हैं। तकनीक के स्तर पर देखें तो DDoS हमलों से बैंकिंग सर्वर ठप कर दिए जाते हैं, API की कमजोरियों से डेटा चोरी होता है और थर्ड पार्टी वेंडर के जरिए पूरे नेटवर्क में सेंध लग जाती है। इस खतरे को देखते हुए RBI ने 2016 में ही Cyber Security Framework लागू किया था। हर बैंक के लिए 24•7 सिक्योरिटी ऑपरेशन सेंटर यानी SOC, नियमित साइबर ऑडिट, और बोर्ड स्तर पर CISO की नियुक्ति अनिवार्य की गई। Master Direction on Digital Payment Security Controls के तहत मल्टी–फैक्टर ऑथेंटिकेशन, डिवाइस बाइंडिंग और रियल टाइम फ्रॉड मॉनिटरिंग को जरूरी बनाया गया। बैंक अब Zero Trust मॉडल पर जा रहे हैं, जहां नेटवर्क के अंदर भी किसी पर

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

आंख बंद करके भरोसा नहीं किया जाता। AI और मशीन लर्निंग की मदद से ग्राहक के ट्रांजैक्शन पैटर्न को समझा जाता है। अगर रात 2 बजे आपके अकाउंट से अचानक दुबई में ₹5 लाख का ट्रांसफर हो, तो सिस्टम तुरंत उसे फ्लैग कर देगा।

2023 में आया डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम यानी DPDP Act इस पूरी लड़ाई में गेम चेंजर साबित हुआ है। अब डेटा लीक होने पर बैंक पर उसके ग्लोबल टर्नओवर का 4 प्रतिशत तक जुर्माना लग सकता है। इस वजह से डेटा एन्क्रिप्शन, डेटा मिनिमाइजेशन और स्पष्ट कस्टमर कंसेंट अब सिर्फ बेस्ट प्रैक्टिस नहीं, कानूनी मजबूरी बन गए हैं। IBA और IDRBT जैसी संस्थाएं भी लगातार नई गाइडलाइंस जारी कर रही हैं ताकि बैंकिंग सेक्टर एक साथ मिलकर खतरों से निपट सके। लेकिन इतनी तैयारी के बाद भी सबसे कमजोर कड़ी आज भी इंसान ही है। दुनिया का सबसे मजबूत फायरवॉल भी फेल हो जाता है अगर ग्राहक खुद फोन पर आए OTP को किसी अनजान व्यक्ति को बता दे। इसलिए तकनीक के साथ–साथ जागरूकता पर निवेश उतना ही जरूरी है। ग्राहक को समझना होगा कि कोई भी बैंक फोन पर OTP, CVV या UPI PIN नहीं मांगता। SMS में आए लिंक पर क्लिक करने की जगह ब्राउजर में अलग से बैंक की साइट खोलें। पब्लिक ॅपथ्प पर नेट बैंकिंग से बचें और सिर्फ ऑफिशियल ऐप स्टोर से ही बैंकिंग ऐप डाउनलोड करें।

आगे की राह साफ है। UPI का दायरा बढ़ रहा है, ब्ठक्ब पायलट से मेनस्ट्रीम की तरफ जा रहा है। इसके साथ ही बैंक अब Passkeys, Behavioral Biometrics और Quantum, safe Encryption जैसी तकनीकों पर काम कर रहे हैं। आने वाले समय में पासवर्ड की जगह आपका टाइपिंग पैटर्न, फोन पकड़ने का तरीका या चेहरा ही आपकी पहचान बनेगा। खतरे भी उतने ही एडवांस होंगे, डीपफेक वॉइस कॉल से लेकर AI आधारित फिशिंग तक। कुल मिलाकर, बैंकिंग में साइबर सिक्योरिटी अब IT डिपार्टमेंट की फाइलों में बंद रिपोर्ट नहीं है। यह ग्राहक, बैंक और रेगुलेटर तीनों की साझा जिम्मेदारी है। टेक्नोलॉजी जितनी स्मार्ट होगी, अपराध भी उतने ही स्मार्ट होंगे। भरोसा ही बैंकिंग की सबसे बड़ी पूंजी है, और उसे बनाए रखने के लिए जागरूकता, निवेश और सहयोग तीनों का संतुलन जरूरी है। अगर हम तीनों मोर्चों पर एक साथ लड़ें, तो डिजिटल इंडिया का यह सफर न सिर्फ तेज, बल्कि सुरक्षित भी रहेगा।

संदर्भ सूची–

1. सरकारी दस्तावेज़ और नीतियाँ

1. भारतीय रिज़र्व बैंक. Cyber Security Framework in Banks. 2 जून 2016. RBI Circular No. RBI/2015-16/418.
2. भारतीय रिज़र्व बैंक. Master Direction on Digital Payment Security Controls. 18 फरवरी 2021.
3. भारत सरकार. डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023. राजपत्र अधिसूचना, 11 अगस्त 2023.
4. भारतीय रिज़र्व बैंक. Annual Report 2024-25. अध्याय IX: Payment and Settlement Systems, पृष्ठ 189-205.

2. रिपोर्ट्स और आंकड़े

5. भारतीय रिज़र्व बैंक. Report on Trend and Progress of Banking in India 2024. दिसंबर 2024.
6. CERT-In. Annual Report 2024: Cyber Security Incidents Handled. इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार.
7. NPCI. UPI Product Statistics & Fraud Trends. 2024-25. http://www.npci.org.in

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 12, December 2025

3. समाचार और लेख

8. “साइबर फ्रॉड के 70% मामले सोशल इंजीनियरिंग से” , दैनिक जागरण, 15 मार्च 2025.
9. “बैंकों पर रैंसमवेयर हमले 35% बढ़े” , इकोनॉमिक टाइम्स हिन्दी, 22 जनवरी 2025.
10. “DPDP Act के बाद बैंकों की जवाबदेही बढ़ी” , बिजनेस स्टैंडर्ड हिन्दी, 5 सितम्बर 2023.

4. तकनीकी संदर्भ

11. भारतीय रिज़र्व बैंक. Booklet on Payment Systems 2024. RBI Publications.
12. IBA & IDRBT. Banking Technology & Cyber Security Guidelines. Indian Banks’ Association, 2023.