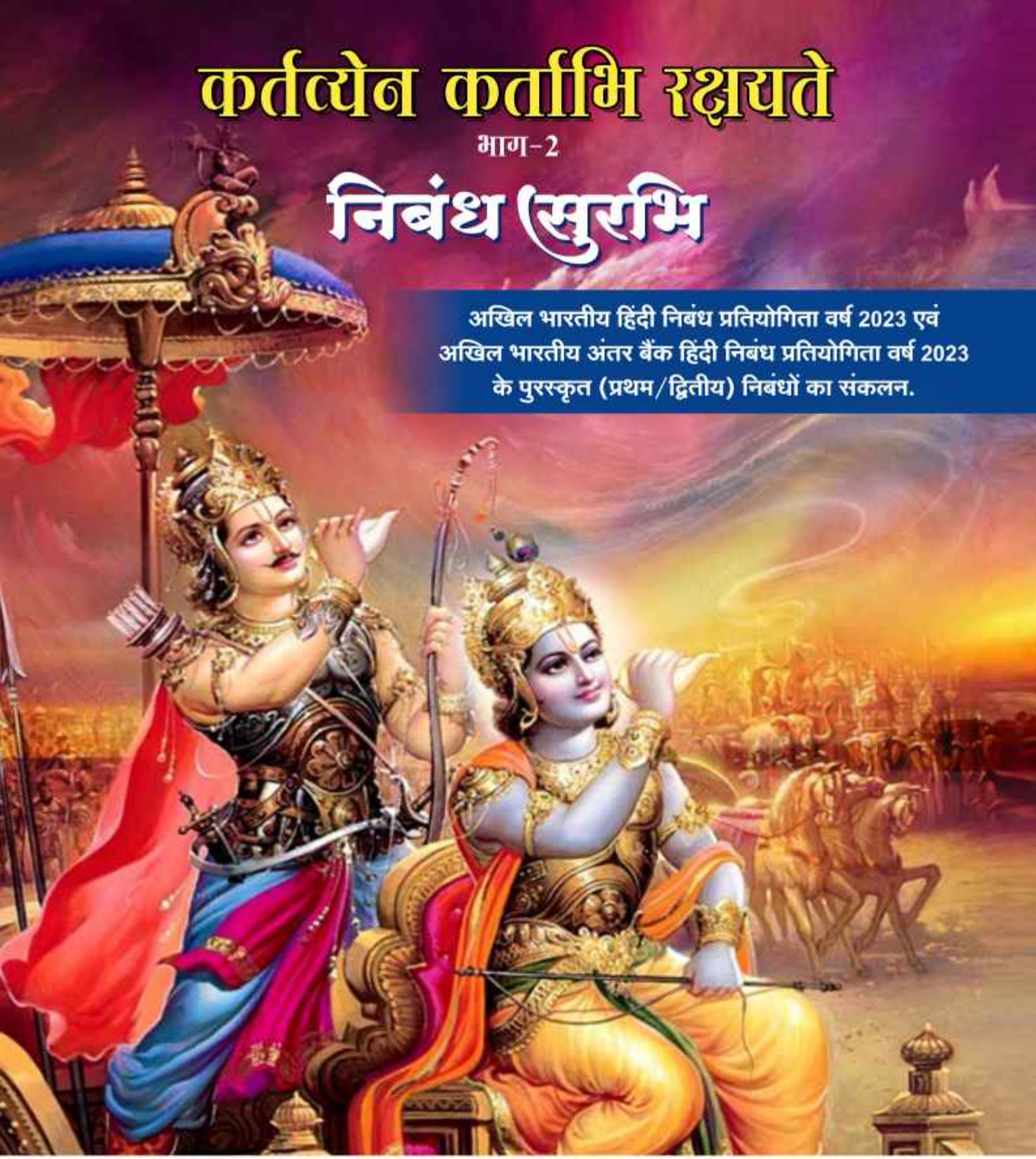
कर्तव्येन कर्ताभि रक्षयते

भाग-2

निबंध सुरभि

अखिल भारतीय हिंदी निबंध प्रतियोगिता वर्ष 2023 एवं
अखिल भारतीय अंतर बैंक हिंदी निबंध प्रतियोगिता वर्ष 2023
के पुरस्कृत (प्रथम/द्वितीय) निबंधों का संकलन.



सेन्ट्रल बैंक ऑफ़ इंडिया
Central Bank of India
1911 से आपके लिए "केंद्रित" "CENTRAL" TO YOU SINCE 1911

राजभाषा विभाग, केन्द्रीय कार्यालय, मुंबई

माँ, मातृभूमि एवं मातृभाषा का
सदैव सम्मान करें,

कार्यालय में राजभाषा एवं
घर में मातृभाषा का प्रयोग करें.

कर्तव्येन कर्ताभि रक्षयते

भाग-2

अनुक्रमणिका

एक हृदय हो भारत जननी!

माननीय प्रबंध निदेशक एवं मुख्य कार्यकारी अधिकारी महोदय का संदेश

प्रिय सेन्ट्रलाइट साथियो,

हार्दिक शुभकामनाएं,

हमारा बैंक भारत सरकार की राजभाषा नीति का सदैव पूरी निष्ठा के साथ अनुपालन कर रहा है परिणामस्वरुप विगत 14 सितंबर 2023 को राजभाषा कीर्ति पुरस्कार प्राप्त हुआ है. इसके अतिरिक्त हमारे बैंक के विभिन्न कार्यालयों को भारत सरकार के क्षेत्रीय कार्यालयों द्वारा निरंतर पुरस्कृत किया जा रहा है.

हमारे बैंक द्वारा अपने सभी संवर्गों के कर्मचारियों को राजभाषा कार्यान्वयन हेतु प्रोत्साहित करने के लिए प्रतिवर्ष विविध प्रकार की रोचक एवं ज्ञानवर्धक हिंदी प्रतियोगिताओं का आयोजन किया जाता है, इसी क्रम में हमारे बैंक द्वारा प्रतिवर्ष अखिल भारतीय अंतर-बैंक (बीमा सहित) हिंदी निबंध प्रतियोगिता का भी आयोजन किया जाता है. हर्ष का विषय यह है कि हमारे बैंक द्वारा आयोजित आखिल भारतीय अंतर-बैंक हिंदी निबंध प्रतियोगिता में विभिन्न बैंकों, बीमा कंपनियों एवं वित्तीय संस्थानों के कर्मचारीगण बड़ी संख्या में सहभागिता करते हैं.

हमारे बैंक द्वारा अपने कर्मचारियों के लिए आयोजित अखिल भारतीय हिंदी निबंध प्रतियोगिता एवं विभिन्न बैंकों एवं वित्तीय संस्थानों के लिए आयोजित अखिल भारतीय अंतर-बैंक हिंदी निबंध प्रतियोगिता के विजेता निबंधों में से कुछ चयनित निबंधों को संकलन के रूप में प्रकाशित करने का उद्देश्य यह है कि अन्य कार्मिक इन निबंधों से ज्ञानार्जन कर लाभान्वित हों.

सुखद भविष्य हेतु मंगल कामनाओं सहित.

एम. वी. राव

प्रबंध निदेशक एवं मुख्य कार्यकारी अधिकारी

* शुभकामना संदेश *

माननीय कार्यपालक निदेशक
श्री विवेक वाही का संदेश

विवेक वाही
कार्यपालक निदेशक

प्रिय साथियो

हिंदी में कार्य हेतु सभी को प्रोत्साहित करने के लिए हमारे केन्द्रीय कार्यालय द्वारा आयोजित (अपने कर्मचारियों हेतु) अखिल भारतीय हिंदी निबंध प्रतियोगिता 2023 एवं विभिन्न वित्तीय संस्थानों बीमा कम्पनियों के कर्मचारियों हेतु आयोजित अखिल भारतीय अंतर-बैंक हिंदी निबंध प्रतियोगिता 2023 के विजयी प्रतिभागियों के चयनित निबंधों के इस संकलन (निबंध सुरभि- खख) कर्तव्येन कर्ताभि रक्षयते के प्रकाशन पर हार्दिक शुभकामनाएं.

* *

माननीय कार्यपालक निदेशक
श्री एम वी मुरली कृष्णा का संदेश

एम वी मुरली कृष्णा
कार्यपालक निदेशक

प्रिय साथियो

हमारे केन्द्रीय कार्यालय द्वारा आयोजित (अपने कर्मचारियों हेतु) अखिल भारतीय हिंदी निबंध प्रतियोगिता 2023 एवं विभिन्न वित्तीय संस्थानों बीमा कम्पनियों के कर्मचारियों हेतु आयोजित अखिल भारतीय अंतर-बैंक हिंदी निबंध प्रतियोगिता 2023 के पुरस्कृत निबंधों के इस ई-संकलन- (निबंध सुरभि- खख) कर्तव्येन कर्ताभि रक्षयते के प्रकाशन पर हार्दिक बधाई.

* *

माननीय कार्यपालक निदेशक
श्री महेंद्र दोहरे का संदेश

महेंद्र दोहरे
कार्यपालक निदेशक

प्रिय साथियो

हिंदी में कार्य करने हेतु सभी को प्रोत्साहित करने के लिए हमारे केन्द्रीय कार्यालय द्वारा आयोजित (अपने कर्मचारियों हेतु) अखिल भारतीय हिंदी निबंध प्रतियोगिता 2023 एवं विभिन्न वित्तीय संस्थानों बीमा कम्पनियों के कर्मचारियों हेतु आयोजित अखिल भारतीय अंतर-बैंक हिंदी निबंध प्रतियोगिता 2023 के विजयी प्रतिभागियों के चयनित निबंधों के इस ई-संकलन (निबंध सुरभि- खख) कर्तव्येन कर्ताभि रक्षयते के प्रकाशन पर सभी को हार्दिक शुभकामनाएं.

* प्रस्तावना *

स्नेही साथियो,

हार्दिक शुभकामनाएं,

भारत के पहले स्वदेशी बैंक सेन्ट्रल बैंक ऑफ इंडिया द्वारा भारत सरकार एवं अन्य संवैधानिक संस्थाओं के दिशा-निर्देशों का पूर्णतः अनुपालन किया जाता है. तदनुसार हमारे बैंक द्वारा भारत सरकार की राजभाषा नीति के अंतर्गत राजभाषा अधिनियम 1963, राजभाषा नियम1976 एवं समय-समय पर जारी विभिन्न निर्देशों का अनुपालन भी किया जाता है.

हमारे बैंक द्वारा नियमित रूप से राजभाषा संगोष्ठियां, राजभाषा सम्मेलन एवं हिंदी कार्यशालाएं आयोजित की जाती है. इसी प्रकार हमारे बैंक के विभिन्न कार्यालय के द्वारा नियमित अंतराल पर विविध प्रकार की हिंदी प्रतियोगिताओं का आयोजन किया जाता है. कई प्रतियोगिताएं तो ऑनलाइन भी आयोजित की जाती हैं, इन प्रतियोगिताओं का उद्देश्य अपने कर्मचारियों को राजभाषा कार्यान्वयन के प्रति प्रेरित और प्रोत्साहित करना है. ऐसे आयोजनों के सदैव सकारात्मक परिणाम प्राप्त होते हैं. इस वर्ष हमारे बैंकों द्वारा अनेक हिंदी प्रतियोगिता के सफल आयोजन के साथ-साथ हमारी लोकप्रिय हिंदी प्रतियोगिता अखिल भारतीय अंतर-बैंक हिंदी निबंध प्रतियोगिता का भी सफलतापूर्वक आयोजन किया गया जिसमें विभिन्न संस्थाओं के कर्मचारियों ने उत्साह पूर्वक सहभागिता की.

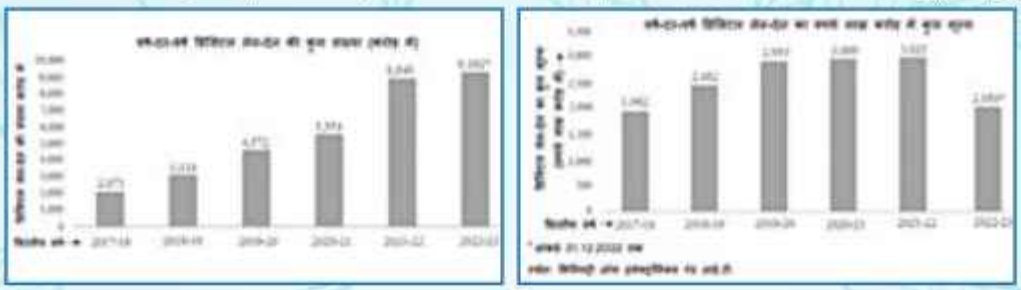
हम विगत कई वर्षों से हमारे बैंक की अखिल भारतीय हिंदी निबंध प्रतियोगिता एवं अखिल भारतीय अंतर-बैंक हिंदी निबंध प्रतियोगिता में चयनित निबंधों का संकलन प्रकाशित करते आ रहे हैं.

इस क्रम में प्रस्तुत है- (निबंध सुरभि-खख) कर्तव्येन कर्ताभि रक्षयते शीर्षक. आशा है पाठकों को यह पसंद आएगा.

सुश्री पॉपी शर्मा
महाप्रबंधक- राजभाषा

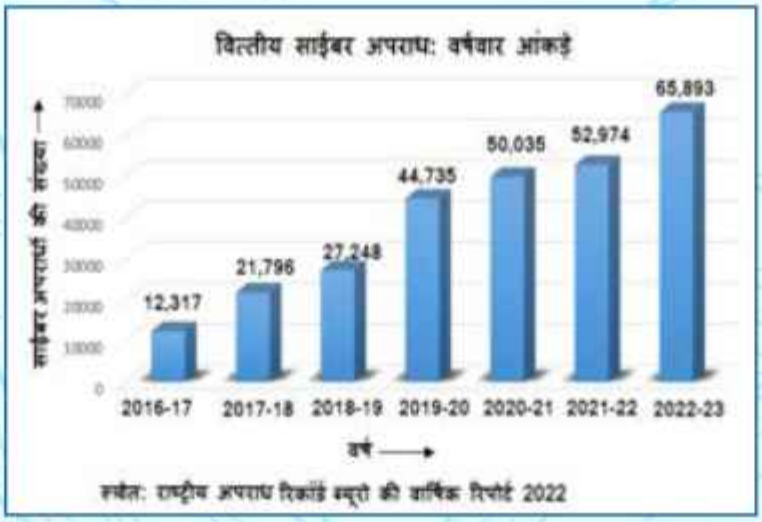
बैंकिंग मे साइबर अपराध

भारत में सूचना–प्रौद्योगिकी पारिस्थितिकी तंत्र के गतिशील और त्वरित विकास ने देश को वैश्विक भुगतान क्षेत्र में एक ताकत के रूप में स्थापित कर दिया है. देश में पहले नोटबंदी और फिर कोरोना महामारी के प्रकोप के दौरान डिजिटल तौर–तरीकों ने लोकप्रियता की नई ऊँचाईयों को छुआ है. सूचना–प्रौद्योगिकी राज्यमंत्री श्री राजीव चंद्रशेखर ने लोकसभा में एक प्रश्न के लिखित उत्तर में बताया है कि देश में वर्ष–दर–वर्ष डिजिटल लेन–देन के परिमाण एवं राशि में निम्नानुसार वृद्धि हुई है:



https://www.pib.gov.in/PressReleasePage.aspx?PRD=1897272

आज हर हाथ में मोबाइल और उँगलियों पर बैंकिंग व्यवहार है, लेकिन जिस तरह हर सिक्के के दो पहलू होते हैं ठीक वही स्थिति डिजिटल लेन–देन के साथ भी है. संप्रति सूचना–प्रौद्योगिकी का उपयोग दोधारी तलवार सिद्ध हो रहा है क्योंकि नित–नए डिजिटल तौर–तरीकों के साथ ही इनसे जुड़े नए–नए प्रकार के साइबर अपराध भी सामने आ रहे हैं. सूचना इस प्रौद्योगिकी युग की नई मूल्यवान आस्ति बन गई है जिसे चुराने के लिए हमारे आस–पास तकनीकी रूप से सक्षम अनेक शातिर अपराधी मौजूद हैं. राष्ट्रीय अपराध रिकॉर्ड ब्यूरो की वार्षिक रिपोर्ट के अनुसार देश में वर्ष–दर–वर्ष वित्तीय साइबर अपराधों के मामले खतरनाक ढंग से बढ़ते ही जा रहे हैं:

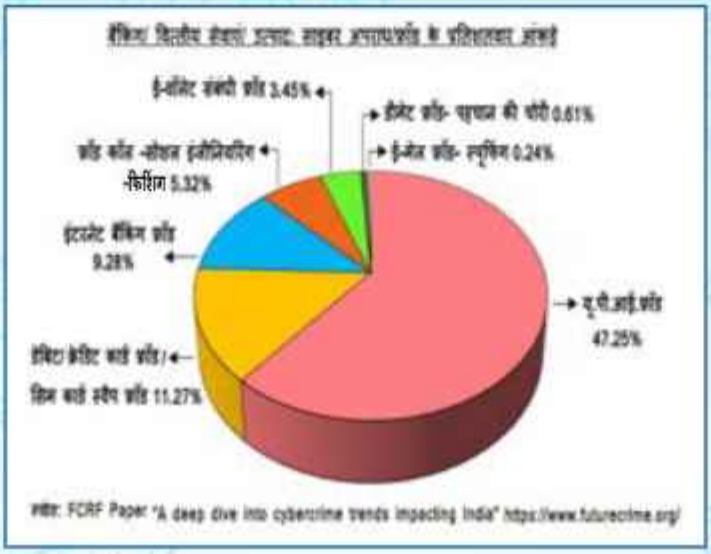


https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf

बैंकिंग क्षेत्र भी साइबर अपराधों के दुष्प्रभावों से अछूता नहीं रह सका है. प्रेस सूचना ब्यूरो द्वारा दिनांक 26–07–2022 को प्रकाशित विज्ञप्ति (https://pib.gov.in/PressReleasePage.aspx?PRID=1845068) के अनुसार गृह राज्यमंत्री श्री अजय मिश्रा ने लोकसभा में जानकारी दी कि भारतीय बैंकों द्वारा रिपोर्ट किए गए साइबर अपराधों के मामले निम्नानुसार रहे:

वित्त वर्ष	साइबर अपराध संबंधी मामलों की संख्या	राशि (रु.करोड़ में)
2020-21	9675	57.06
2021-22	13951	76.49

आई.आई.टी. कानपुर–इनक्यूबेटेड स्टार्ट–अप फ्यूचर क्राइम रिसर्च फाउंडेशन द्वारा सितंबर 2023 में करवाए गए एक अध्ययन में बैंकिंग सेवाओं/ उत्पादों से जुड़े विभिन्न तरह के साइबर अपराधों/ फ्रॉड के निम्नानुसार आंकड़े बताये गए हैं:



साइबर अपराध:

भारतीय संविधान की सातवीं अनुसूची के अनुसार, साइबर अपराध राज्य–सूची के अंतर्गत आते हैं. साइबर अपराध, जिन्हें 'इलेक्ट्रॉनिक अपराध' के रूप में भी जाना जाता है, ऐसे अपराध होते हैं जिनमें अपराध को अंजाम देने के लिए कंप्यूटर या नेटवर्क डिवाइस का उपयोग किया जाता है. साइबर अपराधों को निम्नलिखित तरीकों से वर्गीकृत किया जा सकता है:–

- ऐसे अपराध जिनमें कंप्यूटर को लक्ष्य बनाकर हमला किया जाता है,
- ऐसे अपराध जिनमें कंप्यूटर को एक हथियार के रूप में उपयोग किया जाता है,
- अन्य अपराध जो उपरोक्त वर्गीकरण में पूर्णतः सटीक न बैठते हों.

क. अपराध जिनमें कंप्यूटर को लक्ष्य बनाकर हमला किया जाए:

1. अनाधिकृत पहुँच:

- **हैकिंग:** इसके अंतर्गत किसी व्यक्ति के कंप्यूटर में अनाधिकृत पहुँच बनाई जाती है. हैकर्स पासवर्ड तोड़ने/ भेदने में सक्षम सॉफ्टवेयर्स की सहायता से उपयोगकर्ता की जानकारी के बिना ही उसके सिस्टम पर कई प्रोग्राम इंस्टॉल कर देते हैं. ऐसे प्रोग्राम का उपयोग पासवर्ड और क्रेडिट कार्ड जैसी जानकारियां चुराने के लिए किया जाता है. हैकर्स ग्राहकों के बैंक खातों के अलावा उनके अन्य वित्तीय साधनों जैसे डीमेट खातों आदि को भी लक्षित करते हैं. जुलाई 2020 के दौरान हैकर्स ने अमेरिका के करीब 7.5 मिलियन (डेव) बैंकिंग एप उपयोगकर्ताओं का डाटा हैक कर लिया था.
- **रिमोट एक्सेस:** ग्राहक को उसके मोबाइल /कंप्यूटर पर लुभावने एप्लिकेशन जैसे एनीडेस्क एप आदि डाउनलोड करने का प्रलोभन दिया जाता है. एप्लिकेशन डाउनलोड करते ही उस डिवाइस का नियंत्रण जालसाज़ों के हाथों में आ जाता है और ग्राहक साइबर ठगी का शिकार हो जाता है.
- **जूस जैकिंग:** जब कोई व्यक्ति किसी सार्वजनिक स्थल जैसे एयरपोर्ट आदि पर मौजूद चार्जिंग पॉइंट में मोबाइल चार्ज करने यू.एस.बी. केबल लगाता है तो हैकर्स उस केबल के माध्यम से फोन में कपटपूर्ण सॉफ्टवेयर इंस्टॉल कर देते हैं, जिसके बाद फोन की सभी जानकारियां उन तक पहुँच जाती हैं.

2. मैलेशियस सॉफ्टवेयर अर्थात मैलवेयर:

- **वाईरस:** वाइरस अर्थात वाईटल इन्फर्मेशन रिसोर्सेस अंडर सीज़ ऐसा प्रोग्राम होता है जो फ़ाइलों या कंप्यूटर की हार्ड–ड्राइव को संक्रमित करता है. Q-Bot वाईरस ने वर्ष 2022 के दौरान अनेक बैंकों को प्रभावित किया था.
- **वर्म:** एक दुर्भावनापूर्ण प्रोग्राम जो तेज़ी से स्वयं की प्रतिकृति बना कर स्वचालित रूप से अन्य फ़ाइलों/ प्रोग्रामों को प्रभावित करता है. Ramnit वर्म इन दिनों कई अमेरिकी और ब्रिटिश बैंकों को प्रभावित कर रहा है.
- **स्पाईवेयर:** यह उपयोगकर्ता की वित्तीय/ व्यक्तिगत जानकारियां एकत्रित कर सॉफ्टवेयर बनाने वाले को भेज देते हैं. स्पाइवेयर, बैंकिंग दस्तावेज़ चोरी करने व धोखाधड़ी गतिविधियों के लिए उपयोग किया जाता है. SpyEye ऑनलाइन बैंकिंग को प्रभावित करने वाला एक कुख्यात स्पाईवेयर है.
- **लॉजिक बम:** मैलवेयर जो विशिष्ट शर्तों के पूरा होने तक निष्क्रिय रहता है और ट्रिगर हो जाने पर विनाशकारी कार्रवाई को

अंजाम देता है जैसे फ़ाइलें मिटा देना या प्रणाली को बाधित करना आदि.

- **रैनसमवेयर:** फिरौती मांगने वाला मैलवेयर है जो किसी कंप्यूटर सिस्टम की सभी फाइलों को एनक्रिप्ट कर देता है और फिर धमकी देता है कि यदि फिरौती नहीं चुकाई तो गई तो वह उन सभी फाइलों को करप्ट कर देगा. इंडस्ट्रियल एंड कमर्शियल बैंक ऑफ चाईना (ICBC) नवंबर 2023 में लॉकबिट रैनसमवेयर हमले की चपेट में आ गया था.
- **ट्रोजन हार्स:** मैलवेयर जो अपनी पहचान छुपाकर कंप्यूटर/ डिवाईस में घुसपैठ करता है और फिर उसकी कार्य-प्रणाली को पूर्णत: बाधित कर देता है. गत वर्ष भारतीय बैंकिंग पटल पर ट्रोजन 'सोवा' के फैलने की घटनाएँ सुर्ख़ियों में थीं.

3. सेवाओं में बाधा:

- **सेवा से इनकार (डिनायल ऑफ सर्विस):** इस अपराध के तहत बॉटनेट्स सॉफ्टवेयर की सहायता से किसी सर्वर/ वेबसाइट को डाउन कर दिया जाता है. बॉटनेट्स, हैक किये गए कंप्यूटर के नेटवर्क होते हैं जो अपराधियों द्वारा बाहरी रूप से नियंत्रित किए जाते हैं. DDoS अर्थात डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस इन्हीं हमलों का अधिक परिमार्जित रूप होते हैं जिससे बड़े पैमाने पर सेवाएं ग्राहकों के लिए अनुपलब्ध हो जाती हैं. फरवरी 2022 में रूसी बैंक Sberbank DDoS की चपेट में आ गया था जिससे उसकी वेबसाइट घंटों ऑफलाइन रही थी.
- **इन्फ्रास्ट्रक्चर हमले:** परिष्कृत सॉफ्टवेयर द्वारा डिजिटल प्रमाणपत्र और क्रिप्टोग्राफिक कुंजी जैसे विश्वसनीय बुनियादी घटकों पर हमले किये जाते हैं. इसमें राउटर स्तर के हमले भी शामिल होते हैं जिसके फलस्वरूप सेवाओं तथा संचार आदि में बाधा उत्पन्न होती है.

4. डाटा की चोरी/ छेड़छाड़:

- **मध्य में आदमी हमला (मैन-इन-दि मिडिल):** डाटा चोरी का वह तरीका जो स्निफर, की-लॉगर जैसे सॉफ्टवेयर की सहायता से किया जाता है. अप्रैल 2023 में साइबर जालसाजों ने 'मैन-इन-दि-मिडिल' तरीके से मुंबई की एक कंपनी को 54 लाख रुपये का चूना लगाया था (https://timesofindia.indiatimes.com/city/mumbai/man-in-middle-cons-mumbai-firm-of-rs-54-lakh-with-fake-mail/articleshow/99226594.cms)
- **आईडेंटिटी थेफ्ट (पहचान की चोरी):** अर्थात जालसाज द्वारा किसी व्यक्ति की पहचान (यूज़र आई.डी. व पासवर्ड) या उसके इलेक्ट्रॉनिक हस्ताक्षर आदि चुरा लेना. इसमें उपयोगकर्ता की अनुमति/ जानकारी के बिना उसकी व्यक्तिगत/ वित्तीय जानकारी हासिल करना भी शामिल होता है.
- **इनसाइडर साइबर:** ऐसे अपराध संगठन के कर्मचारियों द्वारा कार्यालय के नेटवर्क-एक्सेस अधिकारों के दुरुपयोग अथवा उपकरणों के गलत इस्तेमाल द्वारा अंजाम दिए जाते हैं. उदा. सलामी अटैक अपराध में कर्मचारी ऐसा प्रोग्राम बैंक सर्वर में डाल देते हैं जिससे हर खाते से इतना कम धन कटे कि वह नजरअंदाज होता रहे लेकिन उस कर्मचारी के पास अच्छी-खासी रकम इकट्ठा हो जाए.

ख. अपराध जिनमें कंप्यूटर को हथियार बनाकर हमला किया जाए:

1.सोशल इंजीनियरिंग: इन अपराधों के अंतर्गत साइबर ठग लोगों में भरोसा पैदा कर, उन्हें लालच देकर या डरा-धमका कर वित्तीय जानकारियां निकलवाने का प्रयत्न करते हैं. इस अपराध की निम्नलिखित श्रेणियों के बारे में हम आए दिन पढ़ते-सुनते रहते हैं:

- विशिंग: यह अपराध टेलीफोन की मदद से किया जाता है जिसमें अपराधियों द्वारा स्वयं को बैंकर या सेवा-प्रदाता बताकर, के.वाई.सी. अद्यतन करने, खाते/ सिम-कार्ड अनब्लॉक करने जैसी बातें कर ग्राहकों की जानकारियां निकलवाई जाती हैं.

- स्पूफिंग: इन अपराधों में जाली प्रेषक पते वाले ई–मेल भेजे जाते हैं. जब ऐसे भ्रामक सन्देश एस.एम.एस. के माध्यम से भेजे जाते हैं तब ये अपराध स्मिशिंग कहलाते हैं. ऐसे मेल/संदेशों में लॉटरी, वसीयत, इनकम–टैक्स रिफंड जैसे प्रलोभनों की आड़ में लोगों से रूपए ऐंठे जाते हैं.
- बेटिंग एंड स्विचिंग: जालसाज़ एक बहुत ही आकर्षक विज्ञापन पोस्ट करता है जो उपयोगकर्ताओं को उस पर क्लिक करने हेतु लुभाता है. जब उपयोगकर्ता विज्ञापन पर क्लिक करता है तो उसे एक कपटपूर्ण पृष्ठ पर रिडायरेक्ट कर दिया जाता है जहाँ वह ठग लिया जाता है.

2.फ़िशिंग: जिस प्रकार मछली पकड़ने के लिए जाल फेंका जाता है, उसी प्रकार लोगों के यूज़र आई.डी. या पासवर्ड चुराने हेतु जालसाज़ों द्वारा लोगों को एक लिंक भेजा जाता है जो हू–ब–हू किसी बैंक/ संस्था का लिंक/ होम–पेज प्रतीत होता है. जब ग्राहक इसमें अपने क्रेडेंशियल्स डालता है तब उसके सारे वित्तीय ब्यौरे अपराधियों तक पहुँच जाते हैं और वह साइबर अपराधियों के जाल में फंस जाता है. दिसंबर 2021 में सिंगापुर ओ.सी.बी.सी. बैंक के अनेक ग्राहक फिशिंग के शिकार बने थे जिससे करीब तेरह मिलियन डॉलर का नुकसान हुआ था.

- एन्क्लर फ़िशिंग हमलों के तहत जालसाज़ शीर्ष कंपनियों के झूठे सोशल मीडिया अकाउंट बनाते हैं और स्वयं को ग्राहक सेवा प्रतिनिधि बताकर लोगों को ठगते हैं.
- व्हेलिंग हमलों में उच्च पदस्थ लोगों जैसे सी.ई.ओ. या सी.एफ.ओ. को लक्षित किया जाता है.
- स्पीयर–फ़िशिंग हमले किसी संगठन के भीतर विशिष्ट व्यक्तियों या समूहों को लक्षित करते हैं.

3.स्पैम एवं स्पिम: स्पैम अनचाही ई–मेल होती हैं तो वहीं स्पिम इंस्टेंट मेसेजिंग एप जैसे वाट्सएप, इन्स्टाग्राम आदि पर आए अनचाहे संदेश होते हैं. इन दोनों के कारण ही सिस्टम की कार्यप्रणाली में बाधा तो उत्पन्न होती ही है साथ ही ये कपटपूर्ण मैलवेयर के वाहक भी होते हैं.

4.यौगिक हमले: विभिन्न हमलों के तरीकों का संयोजन कर साइबर अपराधी और भी अधिक विनाशकारी हमले करते हैं.

अन्य प्रकार के साइबर अपराध:

1.कार्ड संबंधी धोखाधड़ी: यह अपराध गुम/ चोरी हुए कार्ड और कार्ड–क्लोनिंग द्वारा अंजाम दिए जाते हैं. स्किमिंग अपराध में ए.टी.एम./ पी.ओ.एस. कार्ड–स्लॉट पर लगे छोटे से डिवाइस स्किमर की मदद से डेबिट कार्ड विवरण चुराए जाते हैं. पिन की चोरी पिन–होल कैमरे से की जाती है. जालसाजों ने वर्ष 2018 में केनरा बैंक के करीब 300 उपयोगकर्ताओं के ए.टी.एम. विवरण चुराने स्किमिंग तकनीक का प्रयोग कर बैंक खातों से लगभग 20 लाख रुपये की रकम उड़ा ली थी.

2.सिम स्वैप: अपराधी तत्व फर्जी कागजात का इस्तेमाल कर दूरसंचार ऑपरेटर से संपर्क करते हैं और पुराने सिम को निष्क्रिय करवा देते हैं. तत्पश्चात उसी नंबर का नया सिम जारी करवा लेते हैं. सिम स्वैप हो जाने के बाद पीड़ित के वित्तीय संदेशों तक ठगों की पहुंच हो जाती है.

बैंकिंग में साइबर अपराध: कुछ दुष्परिणाम:

बैंकिंग तंत्र में साइबर अपराध के बढते मामले चिंता का विषय बने हुए हुए हैं. ऐसा इसलिए है क्योंकि इन अपराधों के अनेक दुष्परिणाम होते हैं जिनमें छोटी राशि के नुकसान से लेकर देश की वित्तीय स्थिरता के समक्ष गंभीर चुनौती उत्पन होने जैसी विकट समस्याएं शामिल होती हैं:

बैंकिंग में बढते साइबर अपराधों के मुख्य कारण:

विशेषज्ञों ने बैंकिंग में साइबर अपराध के बढ़ते मामलों के पीछे निम्नलिखित कारण बतलाए हैं:

बाधाएं	बैंकिंग प्रणाली में प्रवेश हेतु कम बाधाएं
रुझान	उभरती अपराधिक प्रवृतियां उदा. लालच, प्रतिशोध आदि
मनोवृति	प्रणाली में व्यवधान पैदा करने की इच्छा
प्रौद्योगिकी सीमाएं	विश्लेषणात्मक मॉडलिंग हेतु असमर्थ सिस्टम, धीमी प्रक्रिया
विविध डाटा सोर्स	ग्राहकों / व्यवसाय की सहजता से उपलब्ध जानकारी
कुशलता	परिष्कृत होती तकनीकें
अनुपालन	विनियामक आवश्यकताओं के अनुपालन में शिथिलता

बैंकिंग से जुड़े साइबर अपराध: रोकथाम एवं साइबर सुरक्षा के विभिन्न उपाय:

बैंकिंग में साइबर अपराधों की रोकथाम हेतु सभी पणधारियों जैसे विनियामक अर्थात भारतीय रिज़र्व बैंक, संस्था अर्थात बैंक व कर्मचारियों / ग्राहकों के स्तर पर विभिन्न तौर-तरीके अपनाना अपरिहार्य होता है. आइये चर्चा करें विभिन्न उपायों की जिन्हें अपनाकर साइबर सुरक्षा सुनिश्चित की जा सकती है.

साइबर सुरक्षा के संदर्भ में भारतीय रिज़र्व बैंक द्वारा किए गए उपाय:

- बढते साइबर हमलों के दृष्टिगत आर.बी.आई. ने साइबर सुरक्षा फ्रेमवर्क संबंधी एक व्यापक परिपत्र जारी किया है. परिपत्र में बैंकों को 'साइबर हायजीन' अपनाने की सलाह देते हुए निम्नलिखित मुद्दों पर ज़ोर दिया गया है:

- आर.बी.आई. ने कार्ड स्टोरेज के विकल्प के रूप में Card-on-file Tokenisation अपनाना अनिवार्य कर दिया है. टोकनाइज़ेशन का अर्थ है कार्ड के विवरण को टोकन नामक एक वैकल्पिक कोड के साथ बदलना. टोकनयुक्त कार्ड अधिक सुरक्षित होते हैं क्योंकि लेन-देन के दौरान कार्ड के डाटा कहीं स्टोर नहीं होते.
- 'आर.बी.आई. कहता है' टैगलाइन के तहत Do's . Don'ts टिप्स, साइबर सुरक्षा पर केंद्रित आर.बी.आई. बुकलेट्स जैसे BE(A)WARE- Be Aware and Beware!, राजू और चालीस चोर आदि आम जनता को साइबर अपराधों की रोकथाम के विभिन्न तौर-तरीकों की जानकारी देते हैं.
- डिजिटल लेन-देन से जुड़ी शिकायतें आर.बी.आई. की लोकपाल साईट https://cms.rbi.org.in/ पर या crpcrbi.org.in पर ई-मेल के माध्यम से दर्ज़ करवाई जा सकती हैं (डिजिटल लोकपाल योजना को नवंबर 2021 में एकीकृत लोकपाल योजना में समामेलित कर दिया गया है). गृह मंत्रालय ने भी साइबर फ्रॉड रिपोर्टिंग हेतु हेल्पलाइन नंबर्स 1930 एवं 15526 जारी किए हैं.

संस्था / बैंकों द्वारा किए जा रहे उपाय:

किसी भी संगठन में पी.पी.टी. मॉडल अर्थात पीपुल (लोग), प्रोसेस (प्रक्रिया) एवं टेक्नोलॉजी (तकनीक) को सूचना सुरक्षा का आधार माना जाता है. इसे बैंकिंग परिप्रेक्ष्य में निम्नलिखित तौर पर समझा जा सकता है:

लोग: किसी भी जोखिम का सामना करने संस्था से जुड़े लोग अग्रिम पंक्ति की सुरक्षा की व्यवस्था करते हैं. साइबर जोखिमों

के निवारण में शीर्ष प्रबंधन, बैंक कर्मचारी एवं ग्राहक– इन सभी स्तरों पर जागरूकता का विशेष महत्व है जिसे '3 L': लर्निंग, लेसन एवं लिट्रेसी के रूप में समझ सकते हैं.

प्रक्रिया: बैंक के उच्च प्रबंधन द्वारा सुरक्षा प्रणाली रणनीतियां निम्नलिखित '7 S' को समाहित करते हुए बनाई जाती हैं–

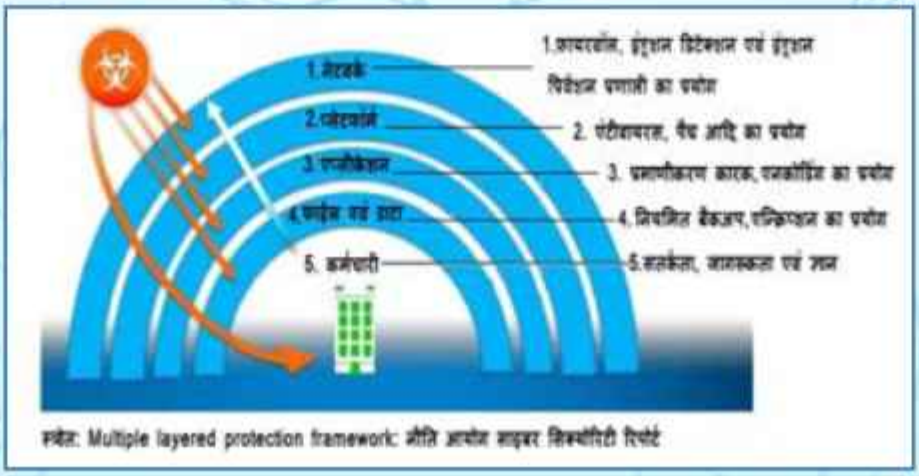
1 S	स्ट्रैटेजी	दीर्घावधि उद्देश्य
2 S	सर्विलैंस	बाह्य/ आंतरिक सतर्कता
3 S	शेयरिंग	अनुभव साझेदारी
4 S	सेंसिटाईजेशन	साइबर जोखिमों के प्रति सभी स्तरों पर जागरूकता
5 S	स्टाफ ओरिएंटेशन	कार्मिक दक्षता एवं क्या करें क्या ना करें आदि का ज्ञान
6 7	सेफगार्डिंग	ग्राहकों के हित और संगठन की प्रतिष्ठा की सुरक्षा
7 S	स्किल	तकनीकी/ परिचालन स्केल का उपयोग

तकनीक: तकनीक में सुरक्षा के '3D' आधार अर्थात डिटर (सी.सी.टी.वी., अलार्म्स), डिटेक्ट (इंट्रूशन डिटेक्शन सिस्टम) व डिनायल (फायरवॉल, एंटीवायरस)को अपनाकर साइबर सुरक्षा सुनिश्चित की जाती है.

भारतीय बैंक पी.पी.टी.मॉडल के इन तीनों तत्वों को समाहित करते हुए विभिन्न उपाय अपना रहे हैं जिनमें उल्लेखनीय हैं:

- बोर्ड अनुमोदित साइबर सुरक्षा नीति का पालन,
- साइबर सुरक्षा ऑडिट,
- हार्डवेयर, सॉफ्टवेयर आदि खरीदते / कनेक्ट करते समय सुरक्षा पहलुओं का आकलन,
- प्रमाणीकरण के दूसरे कारक (2FA) के रूप में ग्राहक के पंजीकृत मोबाइल नंबर पर ओ.टी.पी.,
- पासवर्ड क्रैकिंग से बचाने हेतु ''कैप्चा'',
- फायरवाल, कुकीज़ तथा पैच प्रबंधन व 128/256 बिट एन्क्रिप्शन का उपयोग,
- नियमित बैकअप, डिजास्टर रिकवरी व बिज़नेस कंटीन्यूटी योजना,
- साइबर धोख़ाधड़ी की रिपोर्टिंग हेतु 24X7 ई–मेल, हेल्पलाइन नंबर,
- साइबर सुरक्षा इन्फ्रिन्ज्मेंट (चाहे सफल हों या मात्र प्रयास) की आर.बी.आई. को तत्काल सूचना,
- प्राकृतिक आपदाओं एवं बाहरी तत्वों से मुख्य सर्वर की सुरक्षा,
- बैंक कर्मचारियों हेतु साइबर सुरक्षा संबंधी प्रशिक्षण कार्यक्रमों का संचालन आदि.

भारतीय बैंकों द्वारा साइबर सुरक्षा की इस बहु–स्तरीय कार्ययोजना को नीति आयोग ने अपनी रिपोर्ट में निम्नलिखित रूप में प्रस्तुत किया है:



स्रोत: Multiple layered protection framework: नीति आयोग साइबर सिक्योरिटी रिपोर्ट

साइबर अपराधों की रोकथाम– ग्राहकों एवं कर्मचारियों द्वारा बरती जाने वाली सावधानियां:

डिजिटल बैंकिंग में एंड–यूज़र अर्थात ग्राहक सबसे महत्वपूर्ण कड़ी माने जाते हैं और साइबर सुरक्षा का सबसे कठोर स्तर भी उन्हीं से शुरू होता है. विभिन्न साइबर अपराधों में जो बात प्रमुखता से सामने आती है वह है ग्राहकों का अति–विश्वास, भूल–चूक और लालच जो दर्शाता है कि हमारे देश में साइबर सुरक्षा के बारे में लोगों में विवेक व सतर्कता का अनुपात बहुत ही कम है. साइबर अपराधों की रोकथाम हेतु ग्राहक निम्नलिखित सावधानियां बरतें तो बहुत हद तक सुरक्षित रह सकेंगे:

सामान्य सावधानियां:

- यूज़र–आई.डी. व पासवर्ड डिजिटल दुनिया के प्रवेश–द्वार होते हैं इसलिए उनकी गोपनीयता अत्यंत महत्वपूर्ण है. बैंक का बड़े से बड़ा अधिकारी भी ग्राहकों को यूज़र–आई.डी. एवं पासवर्ड अर्थात यूज़र क्रेडेंशियल बताने हेतु बाध्य नहीं कर सकता. अतः अपने यूज़र क्रेडेंशियल, सीक्रेट प्रश्न, ए.टी.एम. कार्ड, वालेट तथा मोबाइल बैंकिंग के डिटेल्स, ओ.टी.पी.आदि कभी किसी से साझा न करें. याद रखें कि यह जानकारियाँ आपके खाते की कुंजी है जिसकी सुरक्षा आपके अपने हाथों में है.
- यूजर–आई.डी. व पासवर्ड को संग्रह करके रखने हेतु सबसे सुरक्षित स्थान है हमारी खुद की स्मृति. अपनी स्मृति के अलावा अपने यूज़र क्रेडेंशियल और कहीं लिखकर न रखें. विभिन्न डिजिटल सुविधाओं के लिए एक समान यूज़र–आई.डी. व पासवर्ड न रखें. पिन/ पासवर्ड समय–समय पर बदलते रहें.
- मेल/ एस.एम.एस.पर आए लिंक्स की वैधता सत्यापित किए बगैर क्लिक न करें. प्रलोभन देने/ धमकाने वाले संदेशों/ मेल को ब्लॉक कर उसकी रिपोर्ट करें.
- कंप्यूटर/ हैंडसेट की सुरक्षा हेतु एंटी–वायरस एवं एंटी–मैलवेयर का उपयोग करें.
- एस.एम.एस. और ई–मेल द्वारा लेन–देन अलर्ट हेतु पंजीकरण करवाएं. अपने खातों की नियमित जाँच करें और अनियमितता की स्थिति में शाखा से संपर्क करें.

पासवर्ड सुरक्षा:

- हमारा पासवर्ड जितना जटिल होगा उतनी ही हमारी डिजिटल सुरक्षा की दीवार भी मज़बूत होगी. पासवर्ड कम से कम एक संख्या, एक विशेष कैरेक्टर और अपर एवं लोअर केस का मिश्रण हो.
- अपने कंप्यूटर में ऑटो–सेव या रिमेम्बर–मी फ़ंक्शन निष्क्रिय रखें.
- स्मार्टफोन, टैब, कंप्यूटर, लैपटॉप आदि के स्क्रीन–लॉक की गोपनीयता उतनी ही महत्वपूर्ण है जितनी कि यूज़र–आई.डी. व पासवर्ड की.

डिवाईस एवं स्टोरेज सुरक्षा:

- अधिक समय तक उपयोग न होने की स्थिति में इंटरनेट राऊटर/मॉडेम आदि बंद कर दें क्योंकि यही वर्चुअल वर्ल्ड की पहली सीढ़ी हैं.
- डिजिटल बैंकिंग का प्रयोग केवल प्राधिकृत वेबसाईट में ही करें.
- लाइसेंस्ड सॉफ्टवेयर ही प्रयोग करें. पाइरेटेड सॉफ्टवेयर का उपयोग हानि में डाल सकता है.

इंटरनेट/ऑनलाईन बैंकिंग सुरक्षा:

- की–लॉगिंग सॉफ्टवेयर से बचने भौतिक की–बोर्ड की बजाए वर्चुअल की–बोर्ड का उपयोग करें.
- इंटरनेट बैंकिंग सुविधा का उपयोग करने के बाद लॉग–ऑफ करना न भूलें.
- वेरीसाइन व पैडलॉक के चिन्ह सुनिश्चित करें. वेरीसाइन व पैडलॉक के चिन्हों पर क्लिक करके एस.एस.एल. वैधता भी जाँच लें
- एड्रेस बार अर्थात U.R.L. में हमेशा 'https' देखें जहाँ 'S' सिक्योर्ड साईट होना दर्शाता है.
- सार्वजनिक, खुले अथवा शेयर्ड वाई–फाई नेटवर्क पर ऑनलाईन लेन–देन न करें.

ए.टी.एम. सुरक्षा:

- ए.टी.एम. लेन–देन करते समय अपने परिवेश से सावधान रहें. पिन डालते समय की–पैड कवर करें.
- घरेलू और अंतरराष्ट्रीय दोनों तरह के लेन–देन के लिए ई–कॉमर्स प्लेटफॉर्म, पी.ओ.एस. और ए.टी.एम. पर कार्ड लेन–देन सीमा निर्धारित करें.
- पोर्टेबल स्किमिंग उपकरणों से सावधान रहें. ए.टी.एम. इस्तेमाल से पहले ध्यान दें कि मशीन में कुछ असामान्य परिवर्तन जैसे कनेक्टेड एक्सटर्नल डिवाईस आदि तो नहीं हैं?
- कार्ड गुम/ चोरी हो जाए तो तुरन्त कॉल–सेंटर एवं शाखा को रिपोर्ट कर कार्ड हॉटलिस्ट करवा दें.

- पिन और कार्ड एक साथ न रखें और न ही अपना पिन, कार्ड के पीछे लिखें.
- खरीदारी करते समय काउंटर पर सामने कार्ड स्वैप करवा कर तुरंत अपना कार्ड जांच कर वापस लें.
- यदि कोई अजनबी आपके ए.टी.एम. इस्तेमाल करते समय आपकी सहायता करना चाहता है तो उसे इंकार कर दें.

मोबाइल बैंकिंग सुरक्षा:

- मोबाईल हैंडसेट में ऐसी व्यवस्था हो कि फोन चालू करने या स्लीप मोड से सक्रिय मोड में लाने हेतु वह पासवर्ड मांगे। फोन अनलॉक करने पिन/ पासवर्ड या पैटर्न सेट करें. फिंगर-सेंसर/ रेटिना या फेस रिकग्निशन अर्थात बायोमेट्रिक का उपयोग अधिक सुरक्षित है.
- मोबाइल नंबर में परिवर्तन की स्थिति में तत्काल उसे बैंक के साथ अद्यतन कर लें.
- किसी अनजान व्यक्ति को अपना मोबाइल/ टैब/ लैपटाप बिल्कुल न दें क्योंकि हैकर चुटकियों में डाटा चुराने में सक्षम होते हैं.
- मोबाइल गुम या चोरी होने पर फौरन बैंक एवं पुलिस को सूचित करें. उस मोबाइल नंबर के साथ संलग्न सभी बैंकिंग सेवाएं निष्क्रिय करवा दें.
- मोबाइल एप्स विश्वसनीय स्टोर जैसे गूगल प्लेस्टोर/ आई.ओ.एस. स्टोर आदि से ही डाउनलोड करें.
- मोबाइल बैंकिंग एप समय-समय पर अपडेट करते रहें.
- विदेश यात्रा के दौरान घरेलू सिम-कार्ड चालू रखें ताकि बैंक द्वारा भेजे जाने वाली जानकारी निर्विघ्न रुप से मिलती रहे.
- एंड्राइड फोन के नवीनतम ऑपरेटिंग सिस्टम्स (मार्शमेलो/ नौगाट/ ओरियो) में मेसेज, स्टोरेज, कैमरा आदि की अनुमति नियंत्रित कर सकते हैं तथा अवांछित अनुमति बंद कर सकते हैं.
- सार्वजनिक चार्जिंग पॉइंट पर मोबाइल हैण्डसेट चार्ज करने से बचें.
- जरा भी शक हो कि आपके नंबर का इस्तेमाल सिम स्वैपिंग के लिए हो रहा है तो तुरंत इसकी रिपोर्ट अपने मोबाइल ऑपरेटर व बैंक शाखा से करें.
- अनजान आई.एस.डी.नंबर से मिस्ड-कॉल प्राप्त होने पर अपने मोबाइल फोन से उस अंतर्राष्ट्रीय नंबर पर कदापि कॉलबैक न करें.

यू.पी.आई.सुरक्षा:

- कोई भी अज्ञात/ अवांछित यू.पी.आई. लिंक न खोलें.
- मोबाइल पिन और यू.पी.आई. पिन अलग-अलग रखें.
- याद रखें कि राशि ट्रांसफर करने पिन की आवश्यकता होती है, राशि पाने के लिए नहीं.
- अनजान यू.पी.आई. अनुरोधों का जवाब न दें एवं संदिग्ध अनुरोधों को रिपोर्ट करें.

सोशल मीडिया से जुड़ी सावधानियां:

- सोशल मीडिया में आए पॉप-अप मैसेजेस/ लिंक्स पर क्लिक न करें.
- सोशल मीडिया अकाऊंट पर अपने बैंकिंग विवरण या फोन नंबर आदि साझा न करें.
- ओ.टी.पी. मांगने वाले किसी भी व्हाट्सएप/ सोशल मीडिया मैसेज का जवाब न दें.

बैंक कर्मचारी और साइबर सुरक्षा:

- वस्तुत: नेटवर्क एनवायरमेंट में हम उतने ही मज़बूत होते हैं जितनी कि हमारे नेटवर्क की सबसे कमज़ोर कड़ी. बैंक कर्मियों को यह सावधानी बरतनी चाहिए कि वे अपने कामकाज से पूरी की पूरी प्रणाली को संकट में न डाल दें. प्रत्येक कर्मचारी को याद रखना चाहिए कि उसके कंप्यूटर से ही उसकी और उसके संस्थान की सुरक्षा जुड़ी हुई है अतः अनावश्यक रूप से किसी बाहरी व्यक्ति को अपने कंप्यूटर को छूने या प्रयोग करने न दिया जाए.
- यदि किसी कर्मचारी को ऐसा लगता है कि उसने संस्था से संबंधित कोई संवेदनशील जानकारी किसी को दी है तो इसे तुरंत नेटवर्क प्रशासक को बताया जाना चाहिए.
- सभी पासवर्ड नियमित रूप से बदले जाने चाहिए विशेषत: तब, जब उन्हें किसी के सामने प्रकट कर दिया गया हो.
- कंप्यूटर पर कोई भी महत्वपूर्ण प्रलेख, सूचनाएं आदि खुले नहीं छोड़ने चाहिए. कर्मचारी Clear desk, clear screen पॉलिसी का पालन करें.

तो यह तो थे कुछ उपाय जिन्हें अपने दैनंदिन डिजिटल व्यवहार में अपनाकर हम बैंकिंग संबंधी साइबर अपराधों पर लगाम लगा सकते हैं. यहाँ यह भी उल्लेखनीय है कि एक सतर्क ग्राहक एवं जागरूक कर्मचारी को साइबर अपराध का शिकार होने की स्थिति

में अपने अधिकारों, उठाए जाने वाले कदमों और गलत तत्वों को सबक सिखाने का रास्ता भी मालूम होना चाहिए. साइबर अपराधों के शिकार बनने पर तत्काल ही अपराधियों के खिलाफ आई.टी.एक्ट 2000 की धारा–43, 66 और आई.पी.सी.की धारा–420 के तहत साइबर धोखाधड़ी के प्रकरण दर्ज किए जाने चाहिए। कौन जाने कि सतर्कता से उठाया गया एक कदम ही शरारती तत्वों में डर पैदा कर दे, जिससे वह भविष्य में किसी भी व्यक्ति के साथ ऐसी हरकत करने की हिम्मत तक न कर सकें.

बैंकिंग क्षेत्र में साइबर सुरक्षा– कुछ सुझाव:

- बैंकों से अपेक्षित होता है कि वे साइबर सुरक्षा के प्रति जागरूकता फैलाने हेतु नियमित तौर पर डिज़िटल साक्षरता अभियान चलाते रहें. शाखा/ ए.टी.एम परिसर में साइबर सुरक्षा से जुड़े Do's . Don'ts के पोस्टर लगाएं एवं पैम्फलेट का वितरण करें. अशिक्षित/ ग्रामीण ग्राहकों की ओर विशेष ध्यान दें क्योंकि प्रौद्योगिकीय इंटरफेस से भली–भांति परिचित नहीं होने के कारण इनके ठगे जाने का खतरा बढ़ जाता है.
- बैंकों द्वारा डिजिटल लेन–देन से संबंधित एप्स हेतु सिम/ डिवाइस बाइंडिंग को लागू किया जाना चाहिए. डिवाइस बाइंडिंग ग्राहक के डिवाइस को बैंकिंग के लिए एक विश्वसनीय डिवाइस के रूप में पंजीकृत करने की प्रक्रिया होती है.
- साइबर सुरक्षा तंत्र को मज़बूत करने हेतु बैंकों को नवोन्मेषी तकनीकों जैसे मशीन लर्निंग, एल्गोरिदम, व्यवहार विश्लेषण सॉफ्टवेयर, कृत्रिम बुद्धिमता, एंटी–हैकिंग टूल, एक्सेस–कंट्रोल तथा नियम–आधारित पहुँच जैसे नवोन्मेषी क्षेत्रों में शोध एवं निवेश करना चाहिए.
- इनसाईडर थ्रेट से बचाव हेतु बैंकों से अपेक्षित होता है कि वे के.वाई.पी. (अपने भागीदार को जानें) तथा के.वाई.ई. (अपने कर्मचारी को जानें) सिद्धांतों का पालन करें. कर्मचारियों, भागीदारों एवं वेंडरों को स्पष्ट रूप से समझा देना चाहिए कि साइबर सुरक्षित फ्रेमवर्क नीति के उल्लंघन की स्थिति में उन पर कठोर दंडात्मक कार्यवाही की जाएगी.
- बैंक अपने ग्राहकों को साइबर इंश्योरेंस के बारे में जागरूक करें. बजाज एलियांज़ और एच.डी.एफ.सी. अर्गो जैसी बीमा कंपनियां साइबर धोखाधड़ी के प्रकरणों में अपने ग्राहकों को पॉलिसी नियमानुसार मुआवज़ा देती हैं.

बैंकिंग में साइबर सुरक्षा– आगे की राह:

- भविष्य में कृत्रिम बुद्धिमता, डाटा एनालिटिक्स और क्वान्टम कम्प्यूटिंग जैसी तकनीकें साइबर सुरक्षा प्रणालियों की रीढ़ बनकर उभरेंगी. ओ.टी.पी. आधारित अधिप्रमाणन फ्रॉड्स को देखते हुए व्यवहारगत बायोमेट्रिक्स, फेशियल रिकग्निशन तकनीक, डिजिटल टोकन, इन–ऐप अधिसूचना आदि के वैकल्पिक अधिप्रमाणन तंत्र का उपयोग और ज़ोर पकड़ेगा.
- आर.बी.आई. के कार्यकारी निदेशक श्री अनिल शर्मा के अनुसार आर.बी.आई. 'फ्रॉड रजिस्ट्री' (धोखाधड़ी पंजीयक) की स्थापना करने पर विचार कर रहा है. इस रजिस्ट्री की मदद से धोखाधड़ी वाली वेबसाइटों, स्पैम–मेल्स/ कपटपूर्ण कॉलिंग नम्बर्स आदि का डाटा–बेस तैयार किया जाएगा और संदेहास्पद वेबसाइट्स/ फोन नंबर्स आदि को ब्लॉक कर दिया जाएगा.

निष्कर्ष:

बैंकिंग तंत्र में साइबर अपराधों से बचने हेतु आज ग्राहकों को इस प्रकार जागरूक करने की आवश्यकता है कि वह प्रौद्योगिकी का लाभ तो उठाएं पर उसकी सुरक्षा के साथ समझौता कदापि न करें. इस प्रयोजन से बैंकों द्वारा अपने ग्राहकों को ऐसे सरल एवं सुरक्षित डिजिटल समाधान उपलब्ध कराये जाने चाहिए जो भारत में निर्मित और भारत के लिए निर्मित का पर्याय हों. प्रक्रियाओं के पंजीकरण से लेकर साइबर सुरक्षा प्रथाओं तक की सूचनाओं का समझ में आने वाली सरल क्षेत्रीय भाषा या राजभाषा हिन्दी के माध्यम से परिचालित होना अत्यावश्यक है. बैंकिंग में साइबर अपराधों को शून्य तक तो नही लाया जा सकता परंतु विभिन्न उपायों को अपनाकर इन्हें न्यून अवश्य ही किया जा सकता है. बैंकिंग तंत्र को प्रभावित करने वाले विभिन्न साइबर अपराधों से बचाव हेतु यह अत्यावश्यक है कि सभी पणधारी यथा विनियामक, संस्था अर्थात बैंक एवं ग्राहक अपने–अपने स्तरों पर साइबर सुरक्षा की सर्वोत्तम प्रथाओं का कड़ाई से पालन करें और सतर्क रहें, सुरक्षित रहें.

हेयम दु:खम् अनागतम् (अर्थात आने वाले संकट को टाल दें, पूर्वोपाय करें) – (पतंजलि योग सूत्र 2.16)

नौशाबा हसन
सहायक महाप्रबंधक
भारतीय स्टेट बैंक

बैंकिंग मे साइबर अपराध

बैंकिंग क्षेत्र को अर्थव्यवस्था की रीढ़ माना जाता है. हम अपना दैनिक व्यवसाय चलाने के लिए नकदी, चेक और डिमांड ड्राफ्ट का उपयोग करते हैं. रंगराजन समिति (1980) और नरसिम्हा समिति (1991–1998) के सुझाव के बाद आईटी का उपयोग बैंकिंग क्षेत्र में किया गया। बैंकिंग प्रक्रियाओं का कंप्यूटरीकरण और ऑटोमेशन के साथ डिजिटलीकरण किया गया। बैंकिंग उद्योग को आधुनिक बनाए रखने के लिए नवीनतम टेक्नोलॉजी और प्रगतिशील वित्तीय समाधानों का समर्थन किया गया ताकि बैंकिंग सेवाएं और उत्पादों में सुधार किया जा सके और वे उच्चतम ग्राहक संतुष्टि को प्राप्त कर सकें.

अब ग्राहक सीबीएस के कारण कहीं भी, कभी भी बैंकिंग सुविधा का लाभ उठा रहें हैं. बैंक अपने ग्राहकों और उपभोक्ताओं को कई सेवाएँ जैसे ऑनलाइन बैंकिंग, एटीएम डेबिट कार्ड, क्रेडिट कार्ड सेवाएँ, इंटरनेट बैंकिंग और मोबाइल बैंकिंग, टैब् बैंकिंग, फोन बैंकिंग, पीओएस मशीन, सेल्फ सर्विस किओस्क, कैश रिसायकलर इत्यादि डिजिटल बैंकिंग सेवाए प्रदान करते हैं ताकि ग्राहक अपना सारा ट्रांजैक्शन स्वयं कर सकते हैं.

डेबिट कार्ड से ऑनलाइन भुगतान के साथ–साथ ग्राहक दिन के 24 घंटे सभी प्रकार की बैंक सुविधाओं का उपयोग कर सकते हैं. और वे इंटरनेट और सेल फोन का उपयोग करके दुनिया में कहीं से भी आसानी से लेनदेन कर सकते हैं और अपने खाते चला सकते हैं. डेबिट या क्रेडिट कार्ड स्वाइप करने पर आधारित एक नई भुगतान प्रणाली का मार्ग प्रशस्त कर दिया गया है.

सभी जानते हैं कि ये सेवाएँ ग्राहकों के लिए उपयोगी हैं. लेकिन इनका एक स्याह पक्ष भी है. जिसमें साइबर अपराधीं (हैकर्स और डकैतियाँ) शामिल हैं. वे बैंकिंग वेबसाइटों और ग्राहकों के खातों में सेंध लगाकर उन सेवाओं का लाभ उठाते हैं, जिससे खातों में गड़बड़ी होती है और ग्राहकों के खातों से पैसे की चोरी होती है. साइबर अपराधी के पास तकनीकी कौशल होता है जो कंप्यूटर तक पहुंच हासिल करने और अपराध करने के लिए कानून से एक कदम आगे सोचते हैं.

21वीं सदी में साइबर अपराध सबसे घातक प्रतिशोधात्मक हथियार बनकर उभरा है जिसका उपयोग कोई भी व्यक्ति किसी को धमकी देने या धोखा देने के लिए कर सकता है. 2023 की नवीनतम रिपोर्ट के अनुसार भारत में सक्रिय इंटरनेट उपयोगकर्ता लगभग 69.2 करोड़ हैं जो कि भारत के जनसंख्या का 48.7% है. और इस वृद्धि के कारण उपयोगकर्ता के अपराधों के हर दुर्भावनापूर्ण तरीके में फंसने की संभावना पिछले कुछ समय में बढ़ गई है.

साइबर अपराधियों का निशाना इंटरनेट बैंकिंग, ऑनलाइन बैंक खातों पर फिशिंग अटैक और एटीएम/डेबिट कार्ड की क्लोनिंग हैं. ऑनलाइन बैंकिंग और फाइनेंशियल ट्रांजेक्शन के लिए मोबाइल का उपयोग बढ़ने से साइबर अपराध का खतरा और बढ़ गया है.

तेजी से बदलते परिवेश और आईटी उद्योग के महत्वपूर्ण योगदान के मद्देनजर साइबर अपराध एक बड़ी चुनौती है. साइबर–अपराध बड़े पैमाने पर मौद्रिक नुकसान का कारण बनता है. जिसका खामियाजा न केवल ग्राहकों को उठाना पड़ता है. बल्कि बैंकों को भी उठाना पड़ता है. जिससे देश की अर्थव्यवस्था प्रभावित होती है.जब वायरस उत्पन्न होते हैं और अन्य उपकरणों पर फैलते हैं, या जब संवेदनशील व्यावसायिक जानकारी इंटरनेट पर पोस्ट की जाती है. तो गैर–मौद्रिक साइबर अपराध मौजूद होता है.

बैंकिंग उद्योग में साइबर अपराध :

साइबर अपराध का तात्पर्य कंप्यूटर या इंटरनेट पर की गई किसी भी आपराधिक गतिविधि से है. दूसरे शब्दों में डिजिटल कदाचार को साइबर अपराध कहा जाता है जहां अपराधी कंप्यूटर या किसी अन्य इलेक्ट्रॉनिक उपकरणों और इंटरनेट का उपयोग करके अनधिकृत पहुंच के माध्यम से किसी व्यक्ति की निजी सूचनाएं चुराते हैं तथा धन हस्तांतरण और निकासी जैसे कई गलत काम करते हैं.

साइबर अपराध के प्रभाव :

साइबर अपराध का उन लोगों पर दीर्घकालिक परिणाम हो सकता है जिन पर हमला किया जाता है. साइबर हमलावर ऋण लेने,

क्रेडिट हड़पने हैकिंग आदि जैसे साइबर खतरों को अंजाम देते हैं. जिसका बैंकिंग व्यवसाय पर विनाशकारी प्रभाव हो सकता है.

साइबर अपराध के निम्नलिखित प्रभाव हैं:

- वित्तीय क्षति
- गोपनीय जानकारी का उल्लंघन
- कानूनी परिणाम
- पहचान योग्य जानकारी में तोड़फोड़ और चोरी
- प्रतिष्ठा जोखिमों से संपर्क
- परिचालन जोखिम

साइबर अपराध के कारण:

I) डेटा तक आसान पहुंच:

एक बार जब कोई साइबर हमलावर कंप्यूटर सिस्टम में पहुंच प्राप्त करने में सक्षम हो जाता है. तो उनके पास ग्राहकों के निजी वित्तीय दस्तावेजों सहित व्यक्तिगत डेटा तक पहुंच हो सकती है. जिसे कॉपी किया जा सकता है या एक छोटे हटाने योग्य डिवाइस में स्थानांतरित किया जा सकता है.

ii) उपयोगकर्ता की लापरवाही:

कंप्यूटर सिस्टम का उपयोग करने वाले सभी अधिकारियों को कंप्यूटर में संग्रहित अपने गोपनीय डेटा और जानकारी की सुरक्षा के लिए बहुत सावधान और सतर्क रहना चाहिए. पासवर्ड और व्यक्तिगत पहचान संख्या (पिन) के उचित उपयोग के माध्यम से वे पहुंच को सीमित कर सकते हैं. उनकी ओर से कोई भी लापरवाही साइबर अपराधियों को कुछ उपकरणों और रिकॉर्ड तक आसान पहुंच प्रदान करेगी.

iii) संगठनों और बैंकों में आंतरिक नियंत्रण का अभाव:

बैंक अपनी दैनिक गतिविधियों के लिए विभिन्न प्रकार के ऑपरेटिंग सिस्टम का उपयोग करते हैं; इसलिए बैंकों को यह सुनिश्चित करना चाहिए कि उनके पास चालू आंतरिक नियंत्रण और आईटी ऑडिट प्रणालियाँ हैं अन्यथा अकुशल सॉफ्टवेयर और हार्डवेयर प्रणालियों की उपलब्धता के कारण कम्प्यूटरीकृत वातावरण में चूक हो सकती है.

iv) तकनीकी अव्यवस्था:

कई बार बैंकों की तकनीकी अव्यवस्था में कमी होती है, जिससे साइबर अपराधियों को आसानी से सिस्टम में प्रवेश मिलता है.

v) उपयोगकर्ता की लापरवाही: बैंक ग्राहकों की लापरवाही भी एक कारण है, क्योंकि वे अपना खाता सुरक्षित रखने के लिए अनुचित भ्रांतियों में पड़ सकते हैं और फिशिंग या मैलवेयर से प्रभावित हो सकते हैं.

vi) कर्मचारी अपराध:

कई बार, बैंक के कर्मचारी भी अपनी अधिकारिक योजनाओं का दुरुपयोग करके साइबर अपराध कर सकते हैं.

बैंकिंग क्षेत्र से जुड़े साइबर अपराध के प्रकार:

- **हैकिंग:**

  हैकिंग एक साइबर अपराध है जिसमें एक व्यक्ति किसी सिस्टम तक अवैध पहुंच प्राप्त करता है या ग्राहकों के खातों या बैंकिंग साइटों को हैक करके सुरक्षा तंत्र को चकमा देने का प्रयास करता है. हालाँकि, एक हैकर पर धारा 379 और 406 के तहत मुकदमा चलाया जा सकता है और सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 की धारा 66 के साथ पठित धारा 43(ए) के तहत भी मुकदमा चलाया जा सकता है. हैकिंग का अपराध साबित होने पर दोषी को आईटी अधिनियम के तहत तीन साल की जेल या पांच लाख रुपये तक का जुर्माना या दोनों की सजा हो सकती है.

- **कुंजी लॉगिंग (कीस्ट्रोक लॉगिंग) :**
इसे कीस्ट्रोक लॉगिंग या कीबोर्ड कैप्चरिंग कहा जाता है. यह कीबोर्ड पर दबाई गई कुंजी को गुप्त रूप से रिकॉर्ड करने (लॉगिंग) करने की प्रक्रिया है ताकि इसका उपयोग करने वाला व्यक्ति इस बात से बेखबर रहे कि उनकी गतिविधियों पर नज़र रखी जा रही है और ये बैंकिंग विवरण आदि जैसी गोपनीय जानकारी चुराने के लिए अविश्वसनीय रूप से हानिकारक हैं.

- **वायरस और ट्रोजन :**
वायरस एक प्रकार का स्व–प्रतिकृति प्रोग्राम है जो स्वयं की प्रतियां डालकर निष्पादन योग्य कोड या दस्तावेज़ों को संक्रमित करता है. वायरस एक प्रोग्राम है जो एक निष्पादन योग्य फ़ाइल को प्रभावित करता है और संक्रमण के बाद फ़ाइल को असामान्य रूप से व्यवहार करने का कारण बनता है. यह प्रोग्राम फ़ाइलों और ऑपरेटिंग सिस्टम जैसी निष्पादन योग्य फ़ाइलों से जुड़कर फैलता है. निष्पादन योग्य फ़ाइल को लोड करने से वायरस की नई प्रतियां बन सकती हैं. दूसरी ओर, वर्म्स ऐसे प्रोग्राम हैं जो स्वयं की प्रतिकृति बना सकते हैं और पीड़ित के कंप्यूटर से अन्य कंप्यूटरों को प्रतियां भेज सकते हैं. वर्म किसी फ़ाइल को बदलते या हटाते नहीं हैं; इसके बजाय, वे उपयोगकर्ता के कंप्यूटर से अन्य कंप्यूटरों को गुणा और प्रतियां भेजते हैं. ट्रोजन शब्द का उपयोग हैकर्स द्वारा सुरक्षित डेटा में धोखाधड़ी करने के लिए उपयोग की जाने वाली कई खतरनाक युक्तियों को निर्दिष्ट करने के लिए किया जाता है. जब तक इसे कंप्यूटर पर इंस्टॉल नहीं किया जाता, बैंकर ट्रोजन भरोसेमंद सॉफ़्टवेयर जैसा दिखता है. हालाँकि, यह एक दुर्भावनापूर्ण कंप्यूटर एप्लिकेशन है जो ऑनलाइन बैंकिंग सिस्टम द्वारा संसाधित या रखे गए निजी डेटा तक पहुँचने के लिए बनाया गया है. इस प्रकार के कंप्यूटर प्रोग्राम में एक पिछला दरवाजा होता है जो बाहर से कंप्यूटर तक पहुंच को सक्षम बनाता है. दुनिया भर में, 2022 की पहली तिमाही में मोबाइल बैंकिंग ट्रोजन के लिए लगभग 54,000 इंस्टॉलेशन पैकेज थे . पिछले साल की तिमाही की तुलना में 53% से अधिक की वृद्धि हुई है. 2021 की पहली तीन तिमाहियों में गिरावट के बाद, चौथी तिमाही में मोबाइल बैंकिंग को लक्षित करने वाले ट्रोजन पैकेजों की संख्या में वृद्धि हुई थी.

- **मैलवेयर आधारित हमले और रैंसमवेयर :**
इलेक्ट्रॉनिक बैंकिंग सेवाओं के लिए सबसे खतरनाक साइबर खतरों में से एक मैलवेयर–आधारित हमले हैं. ऐसे हमलों में एक दुर्भावनापूर्ण कोड बनाया जाता है. इन दिनों बैंकिंग उद्योग में गैलवैयर हमलों की संख्या बढ़ रही ज़ीउस, स्पाईआई, कार्बप, किन्स और टिनबा, कुछ सबसे प्रसिद्ध बैंकिंग मैलवेयर हैं. लगभग हर वायरस की दो विशेषताएं होती हैं: एक, यह सिस्टम में पिछले दरवाजे से प्रवेश सुनिश्चित करता है. और दूसरा, यह उपयोगकर्ता की क्रेडेंशियल जानकारी चुरा लेता है. यह महत्वपूर्ण डेटा को एन्क्रिप्ट करता है और मालिकों को तब तक उस तक पहुंचने से रोकता है जब तक वे उच्च लागत या फिरौती का भुगतान नहीं करते हैं. चूंकि पिछले वर्ष 90% बैंकिंग संस्थानों को रैंसमवेयर का सामना करना पड़ा है, इसलिए यह उनके लिए एक गंभीर खतरा है. वित्तीय साइबर सुरक्षा के लिए खतरा पैदा करने के अलावा, रैंसमवेयर क्रिप्टोकरेंसी को भी प्रभावित करता है. अपनी विकेंद्रीकृत संरचना के कारण, क्रिप्टोकरेंसी धोखेबाजों को ट्रेडिंग सिस्टम में सेंध लगाने और पैसे चुराने की अनुमति देती है.

- **स्पाइवेयर :**
स्पाइवेयर ऑनलाइन बैंकिंग क्रेडेंशियल्स चुराने और धोखाधड़ी के उद्देश्यों के लिए उनका उपयोग करने का सबसे आम तरीका है. स्पाइवेयर कंप्यूटर और वेबसाइटों के बीच जानकारी एकत्र या प्रसारित करके संचालित होता है. यह अधिकतर सॉफ़्टवेयर डाउनलोड करने के लिए फर्जी 'पॉप अप' विज्ञापनों द्वारा स्थापित किया जाता है. उद्योग मानक एंटीवायरस उत्पाद इस प्रकार के सॉफ़्टवेयर का पता लगाते हैं और उन्हें हटा देते हैं. मुख्य रूप से कंप्यूटर को संक्रमित करने से पहले डाउनलोड और इंस्टॉलेशन को अवरुद्ध करके.

- **फ़िशिंग :**
बैंकिंग क्षेत्र में साइबर सुरक्षा के साथ सबसे आम समस्याओं में से एक फ़िशिंग हमले हैं. उनका उपयोग किसी वित्तीय संस्थान के नेटवर्क में प्रवेश करने और एपीटी (एडवांस्ड पर्सिस्टेंट थ्रेट) जैसे अधिक गंभीर हमले को अंजाम देने के लिए किया जा सकता है, जिसका उन संगठनों पर विनाशकारी प्रभाव पड़ सकता है. एपीटी में, एक

उपयोगकर्ता जिसे अनुमति नहीं है वह सिस्टम तक पहुंच सकता है और लंबे समय तक किसी का ध्यान नहीं जाने पर इसका उपयोग कर सकता है. इससे महत्वपूर्ण वित्तीय डेटा और प्रतिष्ठा हानि हो सकती है. सर्वेक्षण के अनुसार, वित्तीय संस्थानों पर फ़िशिंग हमले 2021 की पहली तिमाही में चरम पर थे.

फ़िशिंग एक प्रकार की धोखाधड़ी है जिसमें निजी जानकारी जैसे डेबिट/क्रेडिट कार्ड नंबर, ग्राहक आईडी, आईपिन, सीवीवी नंबर, कार्ड समाप्ति तिथि इत्यादि ईमेल के माध्यम से चुरा ली जाती है जो वास्तविक स्रोत से आती है. फ़िशिंग त्वरित संदेश और ईमेल स्पूफिंग के उपयोग के माध्यम से की जाती है. इस प्रकार के अपराध में, धोखाधड़ी करने वाले बैंक के अधिकारियों की तरह कार्य करते हैं और वे इस तरह के साइबर हमले में हैकर्स क्लोन साइट का इस्तेमाल करते हैं और एक सीधा लिंक बनाते हैं जो लक्षित ग्राहकों को एक नकली पृष्ठ पर ले जाता है जो वास्तविक बैंक वेबसाइट के समान दिखता है. फिर अर्जित गोपनीय जानकारी का उपयोग ग्राहक के खाते पर धोखाधड़ीपूर्ण लेनदेन करने के लिए किया जाता है.

- **फार्मिंग और स्पूफ़िंग :**

फार्मिंग इंटरनेट के माध्यम से की जाती है. जब कोई ग्राहक किसी बैंक की वेबसाइट पर लॉग इन करता है, तो हमलावर यूआरएल को इस तरह से हाईजैक कर लेते हैं कि वे दूसरी वेबसाइट पर पहुंच जाते हैं.जो झूठी होती है लेकिन बैंक की मूल वेबसाइट की तरह दिखाई देती है. इस तरह के साइबर हमले में हैकर्स क्लोन साइट का इस्तेमाल करते हैं. एक वित्तीय वेबसाइट के रूप में प्रस्तुत करके, वे ; **ऐसा लेआउट डिज़ाइन करते हैं जो दिखने और कार्यक्षमता दोनों में मूल जैसा हो. वर्तनी या डोमेन एक्सटेंशन में मामूली संशोधन के साथ एक डोमेन स्थापित करते हैं .** उपयोगकर्ता इस डुप्लिकेट वेबसाइट को टेक्स्ट या ईमेल जैसी तृतीय-पक्ष संदेश सेवा के माध्यम से एक्सेस कर सकता है. हैकर्स किसी उपयोगकर्ता की लॉगिन जानकारी तक पहुंच सकते हैं जब व्यक्ति ध्यान नहीं दे रहा हो. निर्बाध बहु-कारक प्रमाणीकरण इनमें से कई समस्याओं का समाधान कर सकता है. फ़िशर आजकल ऐसे अपराध करने के लिए एसएमएस (स्मिशिंग) और मोबाइल (वॉयस फ़िशिंग) का भी उपयोग करते हैं.

- **एटीएम स्किमिंग और प्वाइंट ऑफ सेल अपराध :**

वास्तविक कीपैड के रूप में दिखने के लिए मशीन कीपैड के ऊपर एक स्किमिंग डिवाइस स्थापित करना या मशीन के एक हिस्से के रूप में दिखने के लिए कार्ड रीडर पर चिपकाए जाने वाला उपकरण एटीएम मशीनों या पीओएस सिस्टम से समझौता करने की एक रणनीति है. इन उपकरणों पर मैलवेयर भी इंस्टॉल किया जा सकता है जो सीधे क्रेडिट कार्ड डेटा चुराता हैं. एटीएम मशीनों में सफलतापूर्वक स्थापित किए गए स्कीमर व्यक्तिगत पहचान संख्या (पिन) कोड और कार्ड नंबर प्राप्त करते हैं, जिन्हें फिर धोखाधड़ी वाले लेनदेन करने के लिए कॉपी किया जाता है.

- **डीएनएस कैश पॉइज़निंग :**

डीएनएस सर्वर का उपयोग किसी कंपनी के नेटवर्क में पहले प्राप्त क्वेरी परिणामों को कैशिंग करके रिज़ॉल्यूशन प्रतिक्रिया समय बढ़ाने के लिए किया जाता है. डीएनएस सॉफ्टवेयर में खामी का फायदा उठाकर डीएनएस सर्वर पर जहरीले हमले किए जाते हैं. परिणामस्वरूप, सर्वर यह सुनिश्चित करने के लिए गलती से प्राप्त प्रतिक्रियाओं को मान्य कर देता है कि वे एक आधिकारिक स्रोत से हैं. गलत प्रविष्टियाँ सर्वर द्वारा स्थानीय रूप से केश की जाएंगी और समान अनुरोध करने वाले सभी उपयोगकर्ताओं को प्रदान की जाएंगी. बैंक ग्राहकों को अपराधियों द्वारा नियंत्रित सर्वर पर भेजा जा सकता है जिसका उपयोग मैलवेयर परोसने के लिए किया जा सकता है या बैंक ग्राहकों को किसी वैध वेबसाइट की नकली जानकारी प्रदान करने के लिए धोखा दिया जा सकता है. एक हमलावर आईपी एड्रेस को स्पूफ करके ग्राहकों को हाईजैक कर सकता है.

बैंकों पर साइबर अपराध का प्रभाव :

सूचना और प्रौद्योगिकी (आईटी) के विकास के साथ-साथ दैनिक जीवन में मोबाइल नेटवर्क के प्रवेश के परिणामस्वरूप वित्तीय सेवाओं का जनता तक विस्तार हुआ है. हालाँकि, प्रौद्योगिकी प्रगति ने बैंकिंग सेवाओं को सुलभ और किफायती बना दिया है. लेकिन इससे साइबर हमलों का निशाना बनने की संभावना बढ़ गई है.

साइबर चोरों ने न केवल पैसे चुराने के लिए, बल्कि कंपनियों की जासूसी करने और महत्वपूर्ण व्यावसायिक जानकारी तक पहुंच हासिल करने के लिए भी परिष्कृत तरीके विकसित किए हैं, जिसका बैंक के वित्त पर अप्रत्यक्ष प्रभाव पड़ता है. ऐसे साइबर अपराधों से निपटने के लिए बैंकिंग उद्योग को एक मॉडल बनाने के लिए साइबर अधिकारियों और निगरानी संगठनों के साथ काम करना चाहिए जो नियंत्रण में सहायता करेगा.

यहां रुचि का प्रमुख स्रोत बैंकिंग उद्योग में एक कुशल संकलन सेवा की कमी है जो साइबर अपराध में पैटर्न का पता लगा सकती है और उनके आधार पर एक मॉडल संकलित कर सकती है.

भारत में साइबर हमले :

1. **पुणे में कॉसमॉस बैंक पर साइबर हमला**

   पुणे में कॉसमॉस बैंक 2018 में भारत में हाल ही में हुए साइबर हमले का लक्ष्य था, जब हैकर्स ने रुपये चुरा लिए थे। पुणे में स्थित कॉसमॉस कोऑपरेटिव बैंक लिमिटेड से 94.42 करोड़ रुपये की लूट ने भारत में पूरे बैंकिंग उद्योग को हिलाकर रख दिया. हैकर्स ने बैंक के एटीएम सर्वर तक पहुंच हासिल कर ली और बड़ी संख्या में रुपए डेबिट कार्डधारकों और वीजा की निजी जानकारी चुरा ली. पैसा खत्म हो गया और 28 देशों के हैकर गिरोहों ने सूचना मिलते ही धनराशि निकाल ली.

2. **एटीएम सिस्टम हैक**

   कैनरा बैंक के एटीएम सर्वर को 2018 में साइबर हमले के लिए निशाना बनाया गया था. कई बैंक खातों से बीस लाख रुपये साफ कर दिए गए. सूत्रों के अनुसार, साइबर अपराधियों के पास 300 से अधिक उपयोगकर्ताओं की एटीएम जानकारी तक पहुंच थी, जिसके परिणामस्वरूप कुल मिलाकर 50 पीड़ित हुए. हैकर्स ने डेबिट कार्डधारकों से जानकारी हासिल करने के लिए स्किमिंग मशीनों का इस्तेमाल किया. चोरी की गई जानकारी से जुड़े लेन-देन की राशि रुपये से भिन्न थी.

3. **आरबीआई फ़िशिंग घोटाला**

   अपनी तरह के एक साहसिक फ़िशिंग प्रयास में धोखेबाजों ने भारतीय रिज़र्व बैंक को भी नहीं बख्शा। फ़िशिंग ईमेल, जो कथित तौर पर आरबीआई से आया था, ने प्राप्तकर्ता को 48 घंटों के भीतर 10 लाख रुपये की पुरस्कार राशि देने का वादा किया था यदि उन्होंने एक कनेक्शन पर क्लिक किया जो उन्हें एक ऐसी वेबसाइट पर ले गया जो बिल्कुल आरबीआई की आधिकारिक वेबसाइट की तरह दिखती थी, पूर्ण एक ही लोगो और वेब पते के साथ। उसके बाद उपयोगकर्ता से उसका पासवर्ड आई-पिन और बचत खाता नंबर जेसी व्यक्तिगत जानकारी का खुलासा करने के लिए कहा जाता है. दूसरी ओर, आरबीआई ने अपनी आधिकारिक वेबसाइट पर फर्जी फ़िशिंग ई-मेल के बारे में अलर्ट जारी किया.

   भारत में उपरोक्त साइबर हमले पूरी बैंकिंग उद्योग के लिए एक चेतावनी हैं. इसलिए बैंकिंग उद्योग और वित्तिय संगठनों के लिए साइबर सुरक्षा उपायों को अपनाना और सुरक्षा दिशानिर्देशों का पालन करना महत्वपूर्ण है.

साइबर अपराध को रोकने के तरीके:

बैंकिंग उद्योग में अपराधों में चिंताजनक रूप से वृद्धि हुई है जिसके परिणामस्वरूप महत्वपूर्ण आर्थिक नुकसान हुआ है. जैसा कि हम सभी जानते हैं कि बैंकिंग हमारी अर्थव्यवस्था का सबसे महत्वपूर्ण आधार है, इसलिए इसे साइबर हमलों से अवश्य रोका जाना चाहिए. बैंकों और ग्राहकों को इससे जुड़े जोखिम और साइबर हमले से निपटने के लिए सुरक्षा उपायों के बारे में जागरूक किया जाना चाहिए। साइबर सुरक्षा नीति के सभी मामलों के प्रभावी कार्यान्वयन के लिए, सरकार ने राष्ट्रीय सुरक्षा परिषद को नोडल एजेंसी बनाकर एक ''अंतर-विभागीय सूचना सुरक्षा कार्य बल (आईएसटीएफ)'' की स्थापना की है. राष्ट्रीय नोडल एजेंसी ''ईंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम (सीईआरटी-इन)'' है, जिसे कंप्यूटर सुरक्षा घटनाओं के घटित होने पर उनकी जांच करने का काम सौंपा गया है.

साइबर अपराध से जुड़ी मुख्य समस्या क्षेत्राधिकार की है. साइबर अपराध हर राज्य में होता है, इसलिए कोई भी व्यक्ति,

चाहे वह कहीं भी रहता हो, साइबर अपराधों को पहचानने और निगरानी करने में सक्षम होना चाहिए. कुछ मामलों में साइबर अपराध के पीड़ित कई कारणों से साइबर अपराध की रिपोर्ट करने में असमर्थ हो सकते हैं, जैसे दूर के इलाके में रहना, यह अनिश्चित होना कि कहां रिपोर्ट करें और गोपनीयता संबंधी चिंताएँ. एक केंद्रीकृत ऑनलाइन साइबर अपराध निगरानी प्रणाली के अभाव के परिणामस्वरूप, कई साइबर अपराध की घटनाएं दर्ज नहीं की जाती हैं.

आईटी अधिनियम को संशोधित किया जाना चाहिए ताकि साइबर अपराध की परिभाषा के साथ-साथ उन उदाहरणों की सूची भी शामिल की जा सके जिनमें अधिनियम में अलौकिक अधिकार होंगे. भारत में साइबर विनियमन के लिए विधायी आधार को शामिल करने के लिए आईटी अधिनियम के दायरे का विस्तार किया जाना चाहिए. बिचौलियों की जिम्मेदारियाँ अस्पष्ट हैं लेकिन मुझे इसे स्पष्ट करना चाहिए.

बैंकों के लिए शीर्ष साइबर सुरक्षा ढांचा :

एक साइबर सुरक्षा ढांचा विभिन्न देशों और उद्योगों के सुरक्षा नेताओं को उनकी और उनके विक्रेताओं की सुरक्षा स्थितियों को समझने के लिए एक आम भाषा और मानकों का सेट प्रदान करता है. एक रूपरेखा के साथ, साइबर सुरक्षा जोखिम का आकलन, निगरानी और कम करने के लिए आपके संगठन द्वारा अपनाई जाने वाली प्रक्रियाओं और प्रक्रियाओं को परिभाषित करना आसान हो जाता है.

आइए कुछ सामान्य वित्तीय साइबर सुरक्षा ढाँचों पर एक नजर डालें:

1. एनआईएसटी साइबर सुरक्षा ढांचा

पूर्व राष्ट्रपति के कार्यकारी आदेश, क्रिटिकल ईंफ्रास्ट्रक्चर साइबर सुरक्षा में सुधार, ने साइबर जोखिम को पहचानने, विश्लेषण करने और प्रबंधित करने के लिए सार्वजनिक और निजी क्षेत्रों के बीच सहयोग बढ़ाने के लिए कहा. जवाब में, एनआईएसटी साइबर सुरक्षा फ्रेमवर्क बनाया गया था. एनआईएसटी साइबर सुरक्षा परिपक्वता का मूल्यांकन करने, सुरक्षा कमजोरियों का पता लगाने और अनुपालन वैकल्पिक होने पर भी साइबर सुरक्षा कानून का पालन करने के लिए स्वर्ण मानक के रूप में उभरा है. एनआईएसटी अनुपालन प्राप्त करने के लिए, संगठन एनआईएसटी साइबर सुरक्षा ढांचे में उल्लिखित दिशानिर्देशों का पालन कर सकते हैं और यह सुनिश्चित करने के लिए कठोर मूल्यांकन से गुजर सकते हैं कि वे आवश्यक मानकों को पूरा करते हैं.

2. बैंक ऑफ इंग्लैंड का सीबीईएसटी भेद्यता परीक्षण ढांचा

सीबीईएसटी भेद्यता परीक्षण पद्धति यूके के वित्तीय अधिकारियों द्वारा क्रेस्ट (पंजीकृत नैतिक सुरक्षा परीक्षकों के लिए परिषद) और डिजिटल शैडोज़ के सहयोग से विकसित की गई थी. यह एक खुफिया- आधारित परीक्षण ढांचा है. सीबीईएसटी की आधिकारिक शुरुआत 10 जून 2013 को हुई.

सीबीईएसटी किसी विशिष्ट वित्तीय संस्थान के लिए संभावित हमलावरों को खोजने के लिए प्रतिष्ठित वाणिज्यिक और सरकारी स्रोतों से खुफिया जानकारी का लाभ उठाता है. फिर, यह इन संभावित हमलावरों के तरीकों का अनुकरण करता है यह देखने के लिए कि वे संस्था की सुरक्षा को कितनी सफलतापूर्वक तोड़ सकते हैं. यह किसी कंपनी को अपने सिस्टम में कमजोर बिंदुओं की पहचान करने और सुधारात्मक कार्य योजना बनाने और लागू करने में सक्षम बनाता है.

3. निजी तौर पर आयोजित सूचना प्रणालियों के लिए साइबर सुरक्षा और गोपनीयता ढांचा (सिफर फ्रेमवर्क)

कंप्यूटर सिस्टम जो सार्वजनिक और निजी दोनों संगठनों द्वारा नियंत्रित होते हैं और जो अपने ग्राहकों से एकत्र किए गए व्यक्तिगत डेटा को रखते हैं, उन्हें PHIS (प्राइवेटली हेल्ड इंफॉर्मेशन सिस्टम) कहा जाता है. सिफर ढांचा इलेक्ट्रॉनिक प्रणालियों, डिजिटल सूचना प्रकारों और डेटा साझाकरण, प्रसंस्करण और रखरखाव के तरीकों को संबोधित करता है. सिफर कार्यप्रणाली ढांचे का प्राथमिक लक्ष्य निजी तौर पर ऑनलाइन आयोजित सूचना प्रणालियों (पीएचआईएस) की सुरक्षा के लिए प्रक्रियाओं और सर्वोत्तम प्रथाओं का सुझाव देना है. सिफर कार्यप्रणाली ढांचे की मुख्य विशेषताएं निम्नलिखित हैं:

प्रौद्योगिकी स्वतंत्रता (बहुमुखी प्रतिभा) से तात्पर्य किसी भी क्षेत्र में कार्यरत किसी भी संगठन द्वारा उपयोग की जाने वाली

क्षमता से है, भले ही मौजूदा प्रौद्योगिकियां खराब हो रही हों या नई प्रौद्योगिकियों द्वारा प्रतिस्थापित कर दी गई हों. PHIS के मालिक, डेवलपर्स और नागरिक तीन प्रासंगिक उपयोगकर्ता हैं जो इस उपयोगकर्ता-केंद्रित दृष्टिकोण पर ध्यान केंद्रित करते हैं.

व्यावहारिकता – संगठन ऑनलाइन खतरों से डेटा की सुरक्षा कर रहा है या नहीं, इसे बेहतर बनाने या सत्यापित करने के लिए संभावित सावधानियों और नियंत्रणों की रूपरेखा तैयार करता है. इसका उपयोग करना आसान है और इसके लिए व्यवसायों या व्यक्तियों से विशेष ज्ञान की आवश्यकता नहीं है.

साइबर हमले के खतरे को कम करने के तरीके :

1. प्रत्येक कर्मचारी के पास अपना स्वयं का उपयोगकर्ता खाता होना चाहिए. नीति के अनुसार हर तीन महीने में पासवर्ड बदलना आवश्यक है. कर्मचारियों को अनधिकृत सॉफ़्टवेयर डाउनलोड या इंस्टॉल करने की अनुमति नहीं दी जानी चाहिए.
2. सभी कर्मचारियों को अज्ञात स्रोतों से ईमेल अटैचमेंट खोलने या अपलोड करने के खतरों के बारे में सूचित किया जाना चाहिए. संस्थान के बारे में संवेदनशील जानकारी लीक या साझा न करने के महत्व के बारे में कर्मियों को शिक्षित करें.
3. बैंक के आईटी विभाग को यह सुनिश्चित करना चाहिए कि संगठन में प्रत्येक कार्य केंद्र और इंटरनेट से जुड़े डिवाइस पर फ़ायरवॉल सक्षम है क्योंकि फ़ायरवॉल अनधिकृत स्रोतों से सभी संचार को अवरुद्ध करता है.
4. बैंकों को 'दो-कारक प्रमाणीकरण (2FA) ऐप्स या भौतिक सुरक्षा कुंजी का उपयोग करना चाहिए और जहां भी संभव हो, सभी ऑनलाइन खातों पर 2FA सक्षम करना चाहिए.
5. विभाग यह सुनिश्चित करेगा कि सभी पीसी के ऑपरेटिंग सिस्टम को नियमित सुरक्षा अपडेट प्राप्त हों.
6. यह पता लगाने के लिए कि नेटवर्क पर कोई रैंसमवेयर या दुर्भावनापूर्ण सॉफ़्टवेयर है या नहीं, सभी पीसी पर एंटी-स्पाइवेयर और एंटी-वायरस सॉफ़्टवेयर इंस्टॉल होना चाहिए. सभी पासवर्ड और वायरलेस नेटवर्क को सुरक्षित और अच्छी तरह से संरक्षित रखा जाना चाहिए.
7. बैंकों को डायनेगमिक डिवाइस प्रमाणीकरण और वेब-आधारित लेनदेन सत्यापन जैसे सत्यापन तरीकों को नियोजित करना चाहिए क्योंकि अधिक उपभोक्ता मोबाइल उपकरणों का उपयोग करते हैं.
8. ग्राहकों को अपने लेनदेन की वैधता की पुष्टि करने वाले बैंकों से सूचनाएं और स्वचालित संदेश प्राप्त होने चाहिए.
9. ग्राहकों को यह निर्देश दिया जाना चाहिए कि व्यक्तिगत खातों की जानकारी मांगने वाले किसी भी स्रोत की वैधता को कैसे सत्यापित किया जाए. ग्राहकों को बैंक की वेबसाइटों का उपयोग करते समय सुरक्षित रहने के निर्देश भी दिए जाने चाहिए.
10. बैंकिंग एप्लिकेशन या इंटरनेट बैंकिंग का उपयोग करते समय, सुरक्षित नेटवर्क का उपयोग करें.

बैंकों में साइबर सुरक्षा की वर्तमान स्थिति :

जून 2018 और मार्च 2022 के बीच, भारतीय बैंकों ने हैकर्स और अपराधियों द्वारा 248 सफल डेटा उल्लंघनों की सूचना दी; सरकार ने 2 अगस्त, 2022 को संसद को सूचित किया.

भारत सरकार ने 2022 में **11,60,000** साइबर हमलों की सूचना दी है. यह 2019 की तुलना में तीन गुना अधिक होने का अनुमान है. भारत गंभीर साइबर हमलों का लक्ष्य रहा है, जैसे कि फ़िशिंग प्रयास जिसके परिणामस्वरूप लगभग **1419** करोड़ रुपया का धोखाधड़ी वाला लेनदेन हुआ.

ऑनलाइन बैंकिंग से जुड़े साइबर हमले का एक और उदाहरण यूनियन बैंक ऑफ इंडिया था, जिसके परिणामस्वरूप काफी नुकसान हुआ. अधिकारियों में से एक फ़िशिंग ईमेल के झांसे में आ गया और उसने एक संदिग्ध लिंक पर क्लिक कर दिया, जिससे मैलवेयर सिस्टम को हैक कर सका. हमलावर फर्जी आरबीआई आईडी का उपयोग करके सिस्टम में दाखिल हुए.

बैंकों को अपने आईटी जोखिम प्रशासन ढांचे को मजबूत करने का आदेश दिया गया है, जिसमें बोर्ड के अलावा उनके मुख्य सूचना सुरक्षा अधिकारी को सक्रिय भूमिका निभाने का आदेश और बोर्ड की आईटी समिति को आवश्यक मानकों का अनुपालन सुनिश्चित करने में सक्रिय भूमिका निभाना शामिल है.

भारतीय रिज़र्व बैंक (RBI) ने 2022 में **60400 करोड़ रुपये** की बैंक धोखाधड़ी की सूचना दी. 2021 में **100000 करोड़ रुपये** से अधिक की तुलना में, यह गिरावट थी.

ग्लोबल स्तर पर अध्ययन करने वाली रिसर्च फर्म के ताजा सर्वे से पता चलता है कि वित्तीय सेवा क्षेत्र (फाइनेंशियल सर्विसेज सेक्टर) में साइबर अपराध का खतरा सबसे अधिक है.
आँकड़े के अनुसार विगत पाँच साल के धोखाधड़ी की रक़म हैं :

वित्तीय वर्ष	धोखाधड़ी संख्या	आर्थिक रकम (भारतीय रुपया) करोड़
2018–19	6801	73543
2019–20	8703	185450
2020–21	7338	132389
2021–22	9097	59819
2022–23	13530	130000

जैसे–जैसे हम डिजिटल अर्थव्यवस्था की ओर बढ़ रहे हैं, बैंकिंग में साइबर सुरक्षा एक गंभीर चिंता का विषय बनती जा रही है. एक सफल डिजिटल क्रांति के लिए डेटा की सुरक्षा के लिए बनाई गई विधियों और प्रक्रियाओं का उपयोग आवश्यक है. बैंकों में साइबर सुरक्षा की प्रभावशीलता हमारी व्यक्तिगत पहचान योग्य जानकारी (पीआईआई) की सुरक्षा को प्रभावित करती है, चाहे वह अनजाने में हुआ उल्लंघन हो या सुनियोजित साइबर हमला हो.

बैंकिंग और वित्तीय उद्योग में दांव ऊंचे हैं क्योंकि पर्याप्त वित्तीय रकम जोखिम में है और यदि बैंकों और अन्य वित्तीय प्रणालियों से समझौता किया जाता है तो महत्वपूर्ण आर्थिक उथल–पुथल की संभावना है. वित्तीय साइबर सुरक्षा में तेजी से वृद्धि के साथ, साइबर सुरक्षा के पेशे की उच्च मांग है. सर्वोत्तम सुरक्षा प्रमाणपत्रों पर एक नज़र डालें .

बैंकिंग में साइबर सुरक्षा के अनुप्रयोग : कुछ महत्वपूर्ण साइबर सुरक्षा उपकरण हैं:

1. नेटवर्क सुरक्षा निगरानी

नेटवर्क मॉनिटरिंग को खतरनाक या घुसपैठिया व्यवहार के संकेतों के लिए नेटवर्क को लगातार स्कैन करने के रूप में जाना जाता है. इसका उपयोग अक्सर फ़ायरवॉल, एंटीवायरस सॉफ़्टवेयर और आईडीएस (घुसपैठ डिटेक्शन सिस्टम) जैसे अन्य सुरक्षा समाधानों के साथ किया जाता है. सॉफ़्टवेयर मैन्युअल या स्वचालित नेटवर्क सुरक्षा निगरानी की अनुमति देता है.

2. सॉफ्टवेयर सुरक्षा

एप्लिकेशन सुरक्षा उन अनुप्रयोगों की सुरक्षा करती है जो व्यवसाय संचालन के लिए आवश्यक हैं. इसमें लिस्टिंग और कोड हस्ताक्षर की अनुमति देने वाले एप्लिकेशन जेसी सुविधाएं हैं और यह फ़ाइल–साझाकरण अनुमतियों और बहु–कारक प्रमाणीकरण के साथ आपकी सुरक्षा नीतियों को सिंक्रनाइज़ करने में आपकी सहायता कर सकता है. साइबर सुरक्षा में एआई के उपयोग से सॉफ्टवेयर सुरक्षा में अनिवार्य रूप से सुधार होगाा

3. जोखिम प्रबंधन

वित्तीय साइबर सुरक्षा में जोखिम प्रबंधन, डेटा अखंडता, सुरक्षा जागरूकता प्रशिक्षण और जोखिम विश्लेषण शामिल हैं.

जोखिम प्रबंधन के आवश्यक तत्वों में जोखिम मूल्यांकन और उन जोखिमों से होने वाले नुकसान की रोकथाम शामिल है. डेटा सुरक्षा संवेदनशील जानकारी की सुरक्षा को भी संबोधित करती है.

4. महत्वपूर्ण प्रणालियों की सुरक्षा करना

वाइड–एरिया नेटवर्क कनेक्शन बड़े पैमाने पर सिस्टम पर हमलों से बचने में मदद करते हैं. यह उपयोगकर्ताओं द्वारा अपने उपकरणों की सुरक्षा के लिए साइबर सुरक्षा कदम उठाते समय पालन करने के लिए उद्योग द्वारा निर्धारित कठोर सुरक्षा मानकों को कायम रखता है. यह लगातार सभी प्रोग्रामों की निगरानी करता है और उपयोगकर्ताओं, सर्वर और नेटवर्क पर सुरक्षा जांच करता है.

निष्कर्ष

ऑनलाइन लेनदेन की अत्यधिक आसानी, लागत बचत और गति के कारण, भारतीय उपभोक्ता तेजी से ऑनलाइन सेवाओं को पसंद कर रहे हैं. इसके अलावा, वित्तीय संस्थान कम परिचालन लागत के कारण कैशलेस लेनदेन की संख्या बढ़ाने की उम्मीद में उपभोक्ताओं को रोमांचक सौदे पेश कर रहे हैं. ऐसा कहा जा रहा है कि, यह संकेत दिया जा सकता है कि साइबर अपराध से निपटने के लिए आर्थिक संस्थानों की साइबर सुरक्षा पहल एक गतिशील तकनीकी वातावरण और बढ़ते हमलावर कौशल से आगे निकल रही है.

जब कोई व्यक्ति किसी भी प्रकार के इलेक्ट्रॉनिक बैंकिंग लेनदेन में संलग्न होता है, तो साइबर अपराध को रोकने के लिए प्रमाणीकरण, पहचान और सत्यापन तकनीकों को सुनिश्चित करना आवश्यक है. साइबर अपराध के बढ़ने और जांच प्रक्रिया की परिष्कार के लिए पर्याप्त कदम उठाने की आवश्यकता है. साइबर अपराध से निपटने के लिए हितधारक सहयोग में सुधार करना महत्वपूर्ण है.

अपने समग्र परिचालन जोखिम प्रबंधन तंत्र के हिस्से के रूप में, बैंकों को आईटी अधिनियम, 2000 में नवीनतम बदलावों और बैंक लेनदेन से संबंधित जारी किए गए आदेशों, कानूनों, नोटिसों और विनियमों के साथ–साथ इलेक्ट्रॉनिक फंड पर प्रारंभिक कानूनी आवश्यकताओं जैसे निधि अंतरण, इलेक्ट्रॉनिक हस्ताक्षर, डेटा सुरक्षा, डिजिटल हस्ताक्षर और चेक ट्रांजेक्शन को ध्यान में रखना चाहिए.

वित्तीय संस्थान के बैकएंड में उपयोग की जाने वाली प्रौद्योगिकियों के निरंतर सुधार के दौरान, कुछ महत्वपूर्ण पहलुओं को नजरअंदाज कर दिया गया, जिन पर अब तत्काल ध्यान देने की आवश्यकता है. साइबर अपराध की अपनी आकर्षक विशेषताएं हैं जो तेजी से पारंपरिक अपराधों पर भारी पड़ने लगी हैं. साइबर अपराधी गुमनामी के स्तर, वैश्विक पीड़ित तक पहुंच और त्वरित परिणामों जैसे कुछ कारणों से आकर्षित होते हैं. जागरूकता अभियानों की कमी/अपर्याप्तता से साइबर अपराधियों का काम आसान हो जाता है. नवीनतम हमले के तरीकों और दस्तावेजी निवारक कदमों के बारे में जानकारी की कमी के कारण, अनजान ग्राहक आसानी से मूर्ख बन जाते हैं.

साइबर अपराध के बढ़ते प्रभाव के साथ, यह स्पष्ट होता जा रहा है कि स्थानीय कानून प्रवर्तन एजेंसियों के पास साइबर अपराध से जुड़ी घटनाओं की जांच करने के लिए आवश्यक कौशल और संसाधनों की कमी है. प्रशिक्षित साइबर सुरक्षा विशेषज्ञों का उपयोग तेजी से और अधिक सटीक साइबर अपराध जांच परिणाम प्राप्त करने के मामले में एक कदम आगे ले जाता है.

ऐसा माना जाता है कि भारत जैसे विकासशील देशों में तकनीकी विकास से संबंधित इस प्रमुख समस्याओं को हल करने के लिए सभी समस्याओं पर उचित जांच सुनिश्चित करने और अनुमान लगाने और सभी हितधारकों को शामिल करने के बाद, शोध कार्य में उल्लिखित इस प्रकार के जोखिमों को कुछ हद तक कम किया जा सकता है और हम एक तरह से यह सुनिश्चित कर सकते हैं कि भारत डिजिटल रूप से सुरक्षित रहे.

सविता पात्र
प्रबंधक
सेन्ट्रल बैंक ऑफ इंडिया

राजभाषा में एआई (कृत्रिम बुद्धिमत्ता) की भूमिका

भारतीय संविधान की आठवीं अनुसूची में 22 भाषाएँ सूचीबद्ध है, जिन्हें अनुसूचित भाषा के रूप में संदर्भित किया गया है. 14 सितंबर 1949 को देवनागरी लिपि में लिखी गई हिंदी को भारत संघ की राजभाषा के रूप में अपनाया गया.

आर्टिफिशियल इंटेलिजेंस (कृत्रिम बुद्धिमत्ता) कंप्यूटर विज्ञान का एक व्यापक क्षेत्र है जो मशीनों या प्रणालियों को बनाने पर केंद्रित है, जो मानव बुद्धि की आवश्यकता वाले कार्यों को कर सकते हैं. इन कार्यों में सीखना, समस्या सुलझाना, निर्णय लेना, धारणा, प्राकृतिक भाषा को समझना और बहुत कुछ शामिल है. कृत्रिम बुद्धिमत्ता में मशीन लर्निंग, प्राकृतिक भाषा प्रसंस्करण, कंप्यूटर दृष्टि, रोबोटिक्स और विशेषज्ञ प्रणालियों सहित विभिन्न उप–क्षेत्र शामिल हैं.

मशीन लर्निंग (एमएल) कृत्रिम बुद्धिमत्ता का एक उप–समूह है जिसमें मशीनों को डेटा से सीखने और विशिष्ट कार्यों के लिए स्पष्ट रूप से प्रोग्राम किए बिना समय के साथ अपने प्रदर्शन में सुधार करता है. एमएल एल्गोरिदम कंप्यूटर को पैटर्न की पहचान करने, अनुमान करने या डेटा के आधार पर कार्रवाई करने में सक्षम बनाता है. इसमें उन मॉडलों का निर्माण शामिल है जो कार्यों को अधिक सटीक रूप से करने के लिए अनुभव से सीख सकते हैं.

W3टेक के अनुमान के अनुसार, सभी वेबसाइटों में से 63.7 प्रतिशत अंग्रेजी को अपनी सामग्री भाषा के रूप में उपयोग करते हैं. सभी वेबसाइटों में से 0.1% द्वारा हिंदी का उपयोग किया जाता है. शीर्ष 250 यूट्यूब चैनलों में से 66% सामग्री अंग्रेजी में, 15% स्पेनिश में, 7% पुर्तगाली में, 5% हिंदी में, 2% कोरियाई में है, जबकि अन्य भाषाओं में 5% सामग्री है.

कृत्रिम बुद्धिमत्ता से राजभाषा का सशक्तिकरण

पिछले कुछ वर्षों में हिंदी के इंटरनेट उपयोगकर्ताओं की तेजी से वृद्धि देखी गई है. अधिकांश क्षेत्रों में उद्यम आवाज–आधारित इंटरनेट में हिंदी के लगभग एक अरब उपयोगकर्ताओं तक पहुंचने की कोशिश कर रहे हैं, जो कृत्रिम बुद्धिमत्ता, प्राकृतिक भाषा प्रसंस्करण (एनएलपी) और मशीन लर्निंग (एमएल) उपकरणों को तैनात करके तेजी से आगे बढ़ रहा है.

भारत के 1.4 अरब लोगों में से 11% से भी कम लोग अंग्रेजी बोलते हैं. इसलिए कई कृत्रिम बुद्धिमत्ता मॉडल भाषा और भाषा पहचान पर ध्यान केंद्रित करते हैं. गूगल द्वारा वित्त पोषित प्रोजेक्ट वाणी या वॉइस लगभग दस लाख भारतीयों के स्पीच डेटा को इकट्ठा कर रहा है और इसे ऑटोमैटिक स्पीच रिकग्निशन और स्पीच–टू–स्पीच ट्रांसलेशन में इस्तेमाल के लिए ओपन–सोर्सिंग कर रहा है. यह भी राजभाषा में कृत्रिम बुद्धिमत्ता से देश के एक बड़े वर्ग को सहजता प्रदान करेगी.

राजभाषा हिंदी में कृत्रिम बुद्धिमत्ता का एकीकरण डिजिटल विभाजन को पाटने, समुदायों को सशक्त बनाने और भारत के समग्र सामाजिक–आर्थिक विकास में योगदान करने की अपार क्षमता रखता है. केंद्र सरकार ने भाषिनी नामक कृत्रिम बुद्धिमत्ता संचालित अनुवाद प्रणाली के माध्यम से इंटरनेट की भाषा बाधा को तोड़ने की योजना बनाई है. भाषिनी परियोजना भारत में लोगों के इंटरनेट का उपयोग करने के तरीके को पूरी तरह से बदल रही है 1 अंग्रेजी में इंटरनेट सामग्री का उपयोग करने के बजाय, लोग अपनी भाषा में ऐसा करेंगे. भारत की आधी से अधिक आबादी अंग्रेजी में इंटरनेट सामग्री का उपयोग करने में असमर्थ है – वे भाषिनी परियोजना के प्रमुख लाभार्थी होंगे.

विकास चाहे वह आर्थिक, औद्योगिक, सांस्कृतिक, सामाजिक, वैज्ञानिक आदि हो, काफी हद तक अन्योन्याश्रित है. एक राष्ट्र समृद्ध नहीं हो सकता यदि वह केवल एक क्षेत्र में विकसित हो जाता है. किसी राष्ट्र का सर्वांगीण विकास उसके सांस्कृतिक और सामाजिक विकास के बिना प्राप्त नहीं किया जा सकता है. भाषाई विकास सांस्कृतिक और सामाजिक विकास का एक महत्वपूर्ण घटक है. राजभाषा हिंदी वह बंधन है जो हमारी समृद्ध और विविध संस्कृति के मोतियों को बांधता है. इसलिए निरंतर विकास प्राप्त करने के लिए, राजभाषा हिंदी को मजबूत करने की उपेक्षा नहीं की जा सकती है.

भारत में राजभाषा में आर्टिफिशियल इंटेलिजेंस (कृत्रिम बुद्धिमत्ता) का उपयोग तकनीकी एकीकरण और भाषाई विविधता में एक महत्वपूर्ण प्रगति का प्रतीक है. कृत्रिम बुद्धिमत्ता को शासन, प्रशासन, शिक्षा और संचार सहित विभिन्न क्षेत्रों और उद्योगों में उत्तरोत्तर एकीकृत किया गया है. भारत के बहुभाषी परिदृश्य के संदर्भ में, कृत्रिम बुद्धिमत्ता भाषा अनुवाद, पाठ

विश्लेषण, भाषण पहचान और समग्र भाषा संरक्षण की सुविधा में अपार क्षमता रखती है.

मिशन भाषिनी (BHASHINI- BHASHa INterface for India)

भाषिनी को पहली बार वित्त मंत्री के बजट 2021–22 के भाषण में राष्ट्रीय भाषा अनुवाद मिशन (एनएलटीएम) के रूप में उल्लेख मिला था. प्रधानमंत्री की विज्ञान, प्रौद्योगिकी और नवाचार सलाहकार परिषद (पीएम–एसटीआईएसी) द्वारा सिफारिश किए जाने के बाद यह मिशन अस्तित्व में आया. इस मिशन का उद्देश्य यह सुनिश्चित करना है कि जैसे–जैसे और अधिक भारतीय इंटरनेट से जुड़ें, वे अपनी भाषाओं, जिसमें हिंदी भी शामिल है, में वैश्विक सामग्री का उपयोग करने में सक्षम हो. मिशन को औपचारिक रूप से 4 जुलाई को गुजरात के गांधीनगर में डिजिटल इंडिया वीक 2022 के उद्घाटन पर लॉन्च किया गया था. भाषिनी प्लेटफॉर्म आर्टिफिशियल इंटेलिजेंस (AI) और प्राकृतिक भाषा प्रसंस्करण (NLP) संसाधनों को एम्एसएमई (MSME, मध्यम, लघु और सूक्ष्म उद्यम), स्टार्टअप एवं व्यक्तिगत इनोवेटर्स को सार्वजनिक डोमेन में उपलब्ध कराएगा.

अनुवाद उपकरण: भाषिनी मोबाइल एप्लिकेशन, एंड्रॉइड और आईओएस दोनों मोबाइल ऑपरेटिंग सिस्टम पर उपलब्ध है, और वेब सेवा अनुवाद दोनों सहायक और उपयोग में आसान हैं.

भाषिनी पारिस्थितिकी तंत्र में सरकार, शिक्षाविद, अनुसंधान समूह, स्टार्टअप, उद्योग और यहां तक कि नागरिक भी शामिल हैं, जो भारत में भाषाओं के प्राकृतिक भंडार हैं. पारिस्थितिकी तंत्र प्रचुर मात्रा में भाषा डेटा का निर्माण कर रहा है जिसका उपयोग शोधकर्ताओं द्वारा कृत्रिम बुद्धिमत्ता भाषा मॉडल विकसित करने के लिए किया जाता है, जिसके आधार पर स्टार्टअप, उद्योग और सरकार नागरिकों के लिए अभिनव उत्पादों और सेवाओं का निर्माण करते हैं.

भाषिनी की क्षमंता: इस मिशन में ऐसे उपकरण प्रदान किये जा रहे हैं जिनके माध्यम से मशीन आवाज को समझ सकती है, स्वचालित रूप से आवाज को पहचान सकती है, और इसे उस व्यक्ति के लिए अनुवाद कर सकती है जो अन्य भाषा समझता है. व्हाट्सएप और कृत्रिम बुद्धिमत्ता के चैटजीपीटी –3 के साथ प्रयोगात्मक एकीकरण के माध्यम से भाषिनी के तहत एक संवादी कृत्रिम बुद्धिमत्ता विकसित की गई है. भाषिनी व्हाट्सएप चैटबॉट का उपयोग करके, कोई भी अपनी भाषा में एक प्रश्न पूछ सकता है और उसी भाषा में प्रतिक्रिया प्राप्त कर सकता है. इनपुट या तो टेक्स्ट या आवाज हो सकता है और आउटपुट टेक्स्ट और आवाज दोनों के रूप में आता है. वर्तमान में, राजभाषा हिंदी, गुजराती और कन्नड़ भाषाओं में यह सुविधा उपलब्ध है.

चैटजीपीटी – जिसके लॉन्च ने पिछले साल जेनरेटिव कृत्रिम बुद्धिमत्ता में रुचि की लहर को जगाया, वह मुख्य रूप से अंग्रेजी पर प्रशिक्षित है. गूगल बार्ड अंग्रेजी तक सीमित है, और अमेज़ेन का एलेक्सा एप जिन नौ भाषाओं का जवाब दे सकता है, उनमें से एक हिंदी है.

हम सूचना प्रौद्योगिकी और अन्य वैज्ञानिक अनुसंधान के युग में रहते हैं. चाहे वह गांव हो या शहर, उनमें से लंगभग सभी सूचना प्रौद्योगिकी क्रांति से प्रभावित हुए हैं. इन क्षेत्रों में अधिकांश कार्य अंग्रेजी में किया जा रहा है. दूसरी ओर यह भी सच है कि कंप्यूटर आधारित इंटरनेट हिंदी में भी उपलब्ध है. आज गूगल को एक बड़ा खोज इंजन माना जाता है. भले ही गूगल बार्ड अंग्रेजी तक सीमित है परन्तु इसके सर्च इंजन में भी हिंदी की सुविधा उपलब्ध है. वह समझती है कि राजभाषा हिंदी को अपनाए बिना वह भारत में अपनी व्यावसायिक जरूरतों को पूरा नहीं कर सकती. गूगल में निहित कृत्रिम बुद्धिमत्ता राजभाषा को और अधिक सशक्त बनाती है.

कृत्रिम बुद्धिमत्ता और भाषा अनुवाद: भाषा अनुवाद में कृत्रिम बुद्धिमत्ता के एकीकरण ने संचार और पहुंच में क्रांति ला दी है. कृत्रिम बुद्धिमत्ता–संचालित अनुवाद उपकरणों ने राजभाषा बाधाओं को पाटने में महत्वपूर्ण भूमिका निभाई है जिसमे दिनों दिन प्रगति हो रही है. गूगल ट्रांसलेट, माइक्रोसॉफ्ट ट्रांसलेटर और अन्य प्लेटफॉर्म कई भारतीय भाषाओं के बीच टेक्स्ट और आवाज (स्पीच) का अनुवाद करने के लिए कृत्रिम बुद्धिमत्ता एल्गोरिदम का उपयोग करते हैं, समावेशिता को बढ़ावा देते हैं और सूचना प्रसार को सक्षम करते हैं.

शासन: राजभाषा में कृत्रिम बुद्धिमत्ता ने शासन और प्रशासन के एकीकरण को सुव्यवस्थित किया है, जिससे नागरिकों के लिए सेवाएं अधिक सुलभ हो गई हैं. कृत्रिम बुद्धिमत्ता तकनीक से लैस चैटबॉट और आभासी सहायक (वर्चुअल असिस्टेंट)

सरकारी सेवाओं तक पहुंचने में नागरिकों की सहायता करते हैं, विभिन्न क्षेत्रीय भाषाओं में जानकारी प्रदान करते हैं. ये प्लेटफॉर्म प्रश्नों को संभालते हैं, जानकारी प्रदान करते हैं, और प्रक्रियाओं के माध्यम से व्यक्तियों का मार्गदर्शन करते हैं, समग्र नागरिक–सरकार बातचीत को बढ़ाते हैं.

शिक्षा: राजभाषा में कृत्रिम बुद्धिमत्ता ने शिक्षा को भी समावेशी बनाने का कार्य किया है, विशेषकर भाषा अधिग्रहण के लिए 2011 की जनगणना के अनुसार, दस सबसे कम साक्षर राज्यों में से सात हिंदी भाषी राज्य हैं. कृत्रिम बुद्धिमत्ता के उपयोग से साक्षरता दर में वृद्धि की जा सकती है.

1. त्वरित प्रतिक्रिया: कृत्रिम बुद्धिमत्ता से भाषा सीखने वाला ऐप मूल्यांकन कर सकता है और यहां तक कि प्रस्तुत किए जाने के तुरंत बाद स्वचालित रूप से निबंधों का भी मूल्यांकन कर सकता है, त्रुटियों को दिखाकर सुधार का सुझाव दे सकता है. यह छात्र और प्रशिक्षक दोनों के समय को बचाता है.

2. सीखने की प्रक्रिया में व्यस्तता बढ़ाता है: शिक्षार्थी अपने स्वयं के लक्ष्यों को निर्धारित करने, किसी भी समय किसी भी स्थान से अध्ययन करने और भाषा सीखने के लिए एक अनुकूलित पाठ्यक्रम का पालन करने में सक्षम होंगे.

3. भाषा बॉट्स: पहले चैटबॉट का उपयोग केवल समर्थन फंक्शन प्रदान करने के लिए सहायता के लिए किया जाता था। हालांकि, भाषा बॉट भाषा सीखने में नया विकास है. शिक्षार्थी बस भाषा बॉट के साथ बातचीत शुरू कर सकता है और क्रिया में प्रतिक्रिया, युक्तियां और सुधार प्राप्त कर सकता है. डुओलिंगो भाषा बॉट कार्यान्वयन का उत्तम उदाहरण हैं.

4. प्राकृतिक भाषा प्रसंस्करण: कृत्रिम बुद्धिमत्ता शिक्षार्थियों के उच्चारण, व्याकरण और शब्दावली का विश्लेषण करने के लिए प्राकृतिक भाषा प्रसंस्करण (एनएलपी) का उपयोग करके भाषा सीखने में सहायता करता है. यह शिक्षार्थियों को वास्तविक समय में तत्काल प्रतिक्रिया और समर्थन प्रदान करता है.

राजभाषा में कृत्रिम बुद्धिमत्ता की भूमिका के उदाहरण

1. **लीला: आर्टिफिशियल इंटेलिजेंस के माध्यम से भारतीय भाषा अर्जित करना**
2. ये इंटेलिजेंट सेल्फ–ट्यूटरिंग सिस्टम हैं जिनका उपयोग कंप्यूटर या मोबाइल का उपयोग करके ऑनलाइन हिंदी सीखने के लिए किया जा सकता है.
3. **मंत्रा: मशीन सहायक अनुवाद उपकरण:** मंत्रा व्यक्तिगत प्रशासन के निर्दिष्ट डोमेन में अंग्रेजी पाठ का राजभाषा हिंदी में अनुवाद करता है, विशेष रूप से राजपत्र अधिसूचनाएं, कार्यालय आदेश, कार्यालय ज्ञापन और परिपत्र.
4. **सारांशक (सारांशकर्ता):** सारांशक एक प्राकृतिक भाषा आधारित सारांशक है.
5. **वाचांतर:** एक स्पीच–टू–टेक्स्ट ट्रांसलेशन सिस्टम है.
6. **माइक्रोफोन:** उपयोगकर्ता उपयुक्त इनपुट डिवाइस यानी एक माइक्रोफोन के माध्यम से एप्लिकेशन के साथ संवाद करता है. फिर यह मूल राजभाषा हिंदी पाठ में आउटपुट उत्पन्न करता है.
7. **अन्वेषक (द क्वेस्टर):** अन्वेषक (द क्वेस्टर) एक प्राकृतिक भाषा आधारित सूचना पुनर्प्राप्ति प्रणाली है जो एक निश्चित दस्तावेज़ पर पूछे जाने वाले प्रश्न के लिए प्राकृतिक भाषा पाठ में कुशलतापूर्वक और सटीक रूप से स्पष्ट जानकारी प्रदान कर सकती है.

इस प्रकार लीला के माध्यम से संवादात्मक तरीके से राजभाषा हिंदी सीखने, मंत्रा के माध्यम से मौजूदा जानकारी का अनुवाद, सारांश के माध्यम से सारांश, वाचांतर–राजभाषा का उपयोग करके आवाज माध्यम से और अन्वेषक के माध्यम से सूचना पुनर्प्राप्ति के लिए प्रौद्योगिकियां मौजूद हैं.

उपरोक्त सभी में कृत्रिम बुद्धिमत्ता का प्रयोग किया जा रहा है . यहां यह उल्लेख करना महत्वपूर्ण है कि जब अधिकांश सरकारी कार्यालयों में ऑनलाइन काम किया जा रहा है, तो अनुवादित सामग्री को भी ऑनलाइन जांचा जा सकता है जिससे

स्टेशनरी की बचत होती है.

राजभाषा में कृत्रिम बुद्धिमत्ता की शुरूआत और जीवन के विभिन्न पहलुओं में इसका एकीकरण भारतीयों के लिए कई महत्वपूर्ण लाभ प्रदान करता है.

1. भाषा पहुच: कृत्रिम बुद्धिमत्ता राजभाषा हिंदी में संचार की सुविधा प्रदान करता है, भाषा बाधाओं को तोड़ता है और लाखों राजभाषा हिंदी बोलने वालों के लिए जानकारी को अधिक सुलभ बनाता है, जिन्हें अन्य भाषाओं में सामग्री तक पहुचने में चुनौतियों का सामना करना पड़ सकता है.

2. बढ़ी हुई शिक्षा: राजभाषा हिंदी में कृत्रिम बुद्धिमत्ता–संचालित शैक्षिक उपकरण विविध शिक्षण शैलियों को पूरा करते हैं, जिससे व्यक्तियों को सीखने के अनुभव होते हैं. यह शैक्षिक संसाधनों की बेहतर समझ और पहुंच को बढ़ावा देता है, विशेषकर उन लोगों के लिए जो हिंदी के साथ अधिक सहज हैं.

3. बेहतर शासन और सेवाएं: कृत्रिम बुद्धिमत्ता–संचालित प्लेटफार्मों के माध्यम से राजभाषा हिंदी में उपलब्ध सरकारी सेवाएं पहुंच और समावेशिता को बढ़ाती हैं . राजभाषा हिंदी में चेटबॉट और वर्चुअल सहायक नागरिकों को सेवाओं को नेविगेट करने, जानकारी तक पहुंचने और प्रश्नों को हल करने में सहायता करते हैं.

4. आर्थिक अवसर: राजभाषा में कृत्रिम बुद्धिमत्ता एकीकरण तकनीक–संचालित नौकरियों और उद्यमिता के लिए रास्ते खोलता है. यह राजभाषा में कृत्रिम बुद्धिमत्ता–आधारित अनुप्रयोगों और सेवाओं के विकास को प्रोत्साहित करता है, आर्थिक विकास और नवाचार को बढ़ावा देता है.

5. संस्कृति और भाषा का संरक्षण: राजभाषा में कृत्रिम बुद्धिमत्ता हिंदी साहित्य, संस्कृति और भाषा विरासत को संरक्षित करने और बढ़ावा देने में अत्यंत लाभप्रद सिद्ध होगी. यह ऐतिहासिक ग्रंथों को डिजिटाइज़ और संग्रहीत करने, उनकी पहुंच को सुविधाजनक बनाने और भविष्य की पीढ़ियों के लिए उनके संरक्षण को सुनिश्चित करने में सहायता करता है.

6. स्वास्थ्य: राजभाषा हिंदी में कृत्रिम बुद्धिमत्ता–संचालित हेल्थकेयर समाधान स्थानीय भाषा में चिकित्सा जानकारी, टेलीमेडिसिन सेवाएं और स्वास्थ्य संबंधी सलाह प्रदान करते हैं. यह दूरदराज के क्षेत्रों और समुदायों तक जहां हिंदी मुख्य रूप से बोली जाती है, पहुचने में सहायता करता है.

7. रोजगार के अवसर और कौशल विकास: राजभाषा में कृत्रिम बुद्धिमत्ता का एकीकरण कृत्रिम बुद्धिमत्ता से संबंधित क्षेत्रों में कौशल विकास के अवसर प्रदान करता है. कृत्रिम बुद्धिमत्ता प्रौद्योगिकियों पर हिंदी में प्रशिक्षण और शिक्षा व्यक्तियों को विकसित तकनीकी परिदृश्य में संलग्न होने और योगदान करने के लिए सशक्त बनाती है.

8. तकनीकी उन्नति: हिंदी में कृत्रिम बुद्धिमत्ता विकास को प्रोत्साहित करता है. कृत्रिम बुद्धिमत्ता एल्गोरिदम और विशेष रूप से राजभाषा प्रसंस्करण के लिए बनाये गए उपकरणों में नयी खोज को बढ़ावा देता है. यह वैश्विक स्तर पर कृत्रिम बुद्धिमत्ता प्रौद्योगिकी में प्रणति और साथ ही हिंदी को वैश्विक स्तर पर आगे बढ़ाने में योगदान देता है.

9. सामाजिक समावेशिता: राजभाषा में कृत्रिम बुद्धिमत्ता–संचालित अनुप्रयोग सामाजिक समावेशिता को बढ़ावा देते हैं और यह सुनिश्चित करते हैं कि तकनीकी प्रगति समाज के सभी वर्गों को लाभान्वित करती है.

10. डिजिटल साक्षरता में वृद्धि: राजभाषा हिंदी में कृत्रिम बुद्धिमत्ता की शुरुआत हिंदी भाषी समुदायों के बीच डिजिटल साक्षरता को प्रोत्साहित करती है. यह तकनीकी प्रगति के साथ व्यक्तियों को परिचित करता हैं, डिजिटल क्षेत्र में उनकी भागीदारी को बढ़ावा देता है.

वास्तविक दुनिया के अनुप्रयोग

जुगलबंदी एक स्वतंत्र और खुला मंच है जो चैटजीपीटी और भारतीय भाषा अनुवाद मॉडल की शक्ति को जोड़ती है. भविष्य में, जुगलबंदी संभावित रूप से व्हाट्सएप और टेलीग्राम चैटबॉट्स को शक्ति प्रदान कर सकती है ताकि कानूनी जानकारी

तक पहुंच को लोकतांत्रिक बनाने और नागरिकों को गुणवत्तापूर्ण स्वास्थ्य सेवा लाने में मदद मिल सके. इसे माइक्रोसॉफ्ट के मुख्य कार्यकारी सत्या नडेला का भी समर्थन मिला है.

आईआईटी मद्रास में कृत्रिम बुद्धिमत्ता4भारत (AI4Bharat) द्वारा विकसित अनुवाद, बड़े पैमाने पर भारतीय भाषाओं में दस्तावेजों के अनुवाद के लिए एक कृत्रिम बुद्धिमत्ता–आधारित ओपन–सोर्स प्लेटफॉर्म है. यह भाषिनी के लिए डेटा प्रबंधन इकाई के रूप में कार्य करता है.

आगे का मार्ग

भाषिनी के लिए, आवाज भुगतान, बैंकिंग, शिक्षा, स्वास्थ्य देखभाल और खुदरा जैसे क्षेत्रों में आगे बढ़ने का रास्ता है. आवाज पर भाषा अनुवाद पहले से ही एक वास्तविकता है, आवाज का उपयोग करके भुगतान करना भाषिनी के लिए रुचि का विशेष क्षेत्र है . भारत में डिजिटल भुगतान की लोकप्रियता बढ़ रही है और 2023 के अंत तक 135.2 बिलियन डॉलर तक पहुंचने की उम्मीद है.

भारत में सभी खुदरा भुगतान प्रणालियों के लिए एक संगठन, भारतीय राष्ट्रीय भुगतान निगम (एनपीसीआई) कथित तौर पर भारतीय भाषाओं में आवाज–आधारित व्यापारी भुगतान और पीयर–टू–पीयर लेनदेन के लिए एक प्रणाली विकसित करने के लिए ऐआई4भारत (AI4Bharat) के साथ काम कर रहा है. यह फीचर फोन उपयोगकर्ताओं को यूनिफाइड पेमेंट्स इंटरफ़ेस (यूपीआई) जैसे डिजिटल भुगतान नवाचारों से लाभ उठाने में सक्षम करेगा, जो वर्तमान में केवल स्मार्टफोन उपयोगकर्ताओं द्वारा आनंद लिया जाता है. यूपीआई को भाषण–सक्षम बनाने की दिशा में कार्य प्रगति पर है. इसी तरह, भाषिनी वॉयस–आधारित बैंकिग को सक्षम करने के लिए भारतीय रिजर्व बैंक (आरबीआई) के साथ काम कर रही है, और वॉयस–आधारित रिटेल के लिए ओपन नेटवर्क फॉर डिजिटल कॉमर्स (ओएनडीसी) के साथ काम कर रही है.

भाषिनी राष्ट्रीय टेलीमेडिसिन प्लेटफॉर्म ई–संजीवनी को बहुभाषी बनाने पर भी विचार कर रही है. ई–संजीवनी, जो स्मार्टफोन पर चिकित्सा पेशेवरों के लिए त्वरित और सहज पहुंच की सुविधा प्रदान करता है, डिजिटल स्वास्थ्य विभाजन को पाट रहा है. भाषा और साहित्यिक विभाजन को पाटने में मदद करके भाषिनी इसे और ऊपर उठा सकती है.

सरकारी सेवाओं के लिए, भारत का मोबाइल गवर्नेंस ऐप उमंग, जिसे नए युग के शासन के लिए एकीकृत मोबाइल एप्लिकेशन के रूप में जाना जाता है, पहले से ही भाषिनी एपीआई का उपयोग करके प्रत्यक्ष लाभ हस्तांतरण पूरा कर रहा है. वह दिन भी दूर नहीं जब कोई शिकायत निवारण ऐप केंद्रीकृत लोक शिकायत निवारण और निगरानी प्रणाली (सीपीजीआरएएमएस) पर आवाज आधारित शिकायतें करने में सक्षम होगा.

बैंकों हेतु हिंदी में कृत्रिम बुद्धिमत्ता के लाभ

2011 की जनगणना के अनुसार भारत में 43.63% लोग हिंदी बोल सकते हैं. बैंकों के कामकाज में हिंदी के साथ कृत्रिम बुद्धिमत्ता का प्रयोग एक बड़ी आबादी के लिए सहजता प्रदान करेगा. राजभाषा हिंदी में कृत्रिम बुद्धिमत्ता को एकीकृत करना बैंकों को अपने राजभाषा हिंदी भाषी ग्राहकों को अधिक कुशल, व्यक्तिगत और सुरक्षित सेवाएं प्रदान करने का अधिकार देता है, जो ग्राहकों के अनुभव और परिचालन प्रभावशीलता को बढ़ाने में योगदान देता है. ग्राहक अपनी भाषा में बैंक के परिचालन और प्रक्रियाओं को समझ पाएंगे. ऐसा कर वे स्वयं को अधिक सशक्त अनुभव करेंगे. इनमें से प्रमुख निम्नलिखित हैं.

1. बेहतर ग्राहक सेवा: राजभाषा हिंदी में कृत्रिम बुद्धिमत्ता–संचालित चैटबॉट और वर्चुअल सहायक प्रश्नों के त्वरित उत्तर प्रदान करके, सेवाओं के माध्यम से ग्राहकों का मार्गदर्शन करके और हिंदी भाषा में सहायता प्रदान करके ग्राहक सेवा को बढ़ा सकते हैं, इस प्रकार समग्र ग्राहक संतुष्टि में सुधार कर सकते हैं.

2. भाषा अभिगम्यता: कृत्रिम बुद्धिमत्ता–संचालित प्लेटफार्मों के माध्यम से हिंदी में बैंकिंग सेवाओं की पेशकश एक व्यापक ग्राहक आधार तक पहुंच सुनिश्चित करती है, खासकर उन क्षेत्रों में जहां राजभाषा हिंदी मुख्य रूप से बोली जाती है . यह बैंक की पहुंच का विस्तार करता है.

3. व्यक्तिगत बैंकिंग अनुभव: कृत्रिम बुद्धिमत्ता एल्गोरिदम हिंदी में ग्राहक व्यवहार और वरीयताओं का विश्लेषण कर सकते

हैं, जिससे बैंक व्यक्तिगत आवश्यकताओं के अनुरूप व्यक्तिगत सिफारिशों, उत्पादों और सेवाओं की पेशकश कर सकते हैं, जिससे ग्राहक अनुभव बढ़ जाता है.

4. धोखाधड़ी से सुरक्षा: हिंदी में कृत्रिम बुद्धिमत्ता–संचालित सिस्टम से ग्राहक उन धोखाधड़ी की गतिविधियों से बच पायेगा जिनसे वह अंग्रेजी का ज्ञान न होने के कारण फँस जाता है.

5. कुशल डेटा प्रोसेसिंग: कृत्रिम बुद्धिमत्ता बैंकों के लिए भी हिंदी में बड़ी मात्रा में डेट को कुशलता से संभालने में सहायता करता है. राजभाषा हिंदी भाषा के डेटा के आधार पर स्वचालित डेटा प्रोसेसिंग, विश्लेषण और निर्णय लेने से संचालन को सुव्यवस्थित किया जा सकता है, सटीकता में सुधार किया जा सकता है, और बैंकों के लिए बेहतर अंतदृष्टि सक्षम की जा सकती है.

6. जोखिम मूल्यांकन और ऋण अनुमोदन: कृत्रिम बुद्धिमत्ता एल्गोरिदम ऋण से जुड़े जोखिमों का आकलन कर सकते हैं, क्रेडिट इतिहास का विश्लेषण कर सकते हैं, और राजभाषा हिंदी में तेजी से और अधिक सटीक ऋण अनुमोदन निर्णय ले सकते हैं. इससे ग्राहकों के लिए ऋण आवेदन प्रक्रिया में तेजी आती है.

7. अनुपालन और नियामक सहायता: कृत्रिम बुद्धिमत्ता उपकरण राजभाषा हिंदी में विशाल मात्रा में डेटा का विश्लेषण करके और बैंकिंग नियमों के अनुपालन को सुनिश्चित करके नियामक आवश्यकताओं का पालन करने में बैंकों की सहायता कर सकते हैं, जिससे गैर–अनुपालन से संबंधित जोखिम कम हो सकती है.

8. लागत में कमी और दक्षता: राजभाषा हिंदी में कृत्रिम बुद्धिमत्ता के माध्यम से देश में नियमित कार्यों के स्वचालन से बैंकों के लिए परिचालन लागत कम हो सकती है. हिंदी संचालित सिस्टम दोहराए जाने वाले कार्यों को संभाल सकते हैं, जिससे कर्मचारियों को अधिक जटिल मुद्दों पर ध्यान केंद्रित करने और समग्र परिचालन दक्षता में सुधार करने की अनुमति मिलती है.

निष्कर्ष

भारत की राजभाषा में कृत्रिम बुद्धिमत्ता का एकीकरण विभिन्न डोमेन में समावेशिता, पहुंच और दक्षता की दिशा में एक परिवर्तनकारी छलांग का प्रतीक है. इसने राजभाषा को जन जन से जोड़ने का कार्य किया है. जैसे–जैसे प्रौद्योगिकी का विकास जारी है, कृत्रिम बुद्धिमत्ता भाषा मॉडल में प्रगति भाषाई अंतराल को पाटने, सांस्कृतिक आदान–प्रदान को बढ़ावा देने और भारत में सभी भाषाई समुदायों के लिए सूचना और सेवाओं तक समान पहुंच सुनिश्चित करने में महत्वपूर्ण भूमिका निभाएगी। जबकि कृत्रिम बुद्धिमत्ता में बहुत संभावनाएं हैं, भारत में राजभाषा में कृत्रिम बुद्धिमत्ता में इसके एकीकरण को कुछ चुनौतियों का सामना करना पड़ता है. भाषाओं के भीतर बोलियों और बारीकियों में भिन्नता के कारण भाषाई विविधता एक चुनौती है. कृत्रिम बुद्धिमत्ता मॉडल संदर्भ या बोलचाल की सटीक व्याख्या नहीं कर सकते हैं, जिससे अनुवाद में अशुद्धियां हो सकती हैं. इसके अलावा, क्षेत्रीय भाषाओं में डेटा उपलब्धता और गुणवत्ता एक चिंता का विषय बनी हुई है, जो कृत्रिम बुद्धिमत्ता मॉडल के प्रदर्शन को प्रभावित करती है.

इन चुनौतियों से निपटने के लिए ठोस प्रयास किए जा रहे हैं. राजभाषा में कृत्रिम बुद्धिमत्ता अनुसंधान और विकास को बढ़ावा देने वाली सरकारी पहल का उद्देश्य भाषा मॉडल को परिष्कृत करना और सटीकता में सुधार करना है. शिक्षाविदों, उद्योग और नीति निर्माताओं के बीच सहयोग भाषा–विशिष्ट डेटासेट विकसित करने और बेहतर भाषा समझ और अनुवाद के लिए कृत्रिम बुद्धिमत्ता एल्गोरिदम को बढ़ाने पर ध्यान केंद्रित करता है. यह एक ऐसे भारत के निर्माण में मदद कर सकता है जहां ज्ञान सभी के लिए सुलभ हो, जिसमें इसके नागरिक वास्तव में शामिल हों, सशक्त हों, और वास्तविक अर्थों में आत्मनिर्भर हों.

विनीत भारद्वाज
मुख्य प्रबंधक
यूनियन बैंक ऑफ इंडिया

बैंकिंग मे साइबर अपराध

''खल: करोति दुर्वृतं नूनं फलति साधुषु।
दशाननो हरेत सीतां बंधनं स्याद महोदधे: ..''

अर्थात, दुष्ट मानव अनुचित कार्य करता है और उसका फल अच्छे मानव को भुगतना पड़ता है. रावण सीता का हरण करता है और सागर को बंधना पडता है.

एक दिन हमारे कार्यालय के व्हाट्स अप चैट ग्रुप में एक मैसेज आ धमका – सभी से निवेदन है कि श्री अमन, सहायक महाप्रबंधक साहब का मोबाइल नंबर हैक हो गया है. अतः आप उनके नंबर द्वारा मिली पैसों की मांग बिल्कुल स्वीकार न करें. तथा इस सूचना को अन्य कर्मियों तक अग्रेषित करें. सावधानी के तौर पर साहब का नंबर ब्लॉक करने हेतु आवेदन मोबाइल सेवा प्रदाता कंपनी को भेजा गया है. इस मैसेज के साथ इस साइबर अपराध की पुलिस थाने मे दर्ज शिकायत की कॉपी भी संप्रेषित की गयी थी. सुबह कार्यालय में आने के बाद इस घटना के बारे मे विस्तार से पता चला; कि श्री अमन के कुछ अहम दस्तावेज़ कूरियर से आने थे. उसी संदर्भ मे एक कॉल उन्हें प्राप्त हुआ जिसमे सामनेवाले व्यक्ति ने श्री अमन को *# डायल करने के बाद एक नंबर पर कॉल करने को कहा. चूंकि श्री अमन अपने अहम दस्तावेज़ को सही समय पर प्राप्त करना चाहते थे उन्होंने कॉल करने वाले पर विश्वास किया और उसके निर्देशानुसार उस नंबर पर कॉल किया. उस कॉल के दौरान बीच में संपर्क तूट गया और कुछ देर में ही पता चला की श्री अमन के निकटवर्तीयों द्वारा कुल 1 लाख राशि हैकर तक पहुँच गयी है. शायद हमारे लिए यह साइबर अपराध का एक ताजा उदाहरण था जो हमें इस घटना और ऐसे अन्य साइबर अपराधों के बारे में विस्तार से जानकारी लेने हेतु मजबूर करने लगा. मन में विचार आने लगे की, अच्छाईयत और बुराईयत की यात्रा साथ साथ चलती है, इसके प्रमाण सदियों से इतिहास के पन्नों मे मिलते है. सामाजिक व्यवस्था में समाज के सदस्यों के हितों और सुरक्षा को ध्यान में रखते हुए कुछ नियम बनाए जाते हैं. इन नियमों के विपरीत आचरण प्रचलित समाजव्यवस्था के लिए खतरा बन सकता है. इसीलिए नियमों से विपरीत वर्तन को अपराध माना जाता है. अपराध एक अवैध कार्य या गतिविधि है जिसके लिए किसी व्यक्ति को कानून द्वारा दंडित किया जा सकता है. अपराध एक सार्वभौमिक समस्या है जो प्रत्येक समाज में किसी न किसी रूप में पाई जाती है. ईलेक्ट्रोनिक उपकरण इक्कीसवी सदी की सबसे महत्वपूर्ण खोज है जो सूचना और प्रौद्योगिकी क्रांति के शीर्ष साबित हुई है. आज कम्प्यूटर, इंटरनेट, मोबाइल जैसे उपकरण तथा सूचना और प्रौद्योगिकी तकनीक पर मानव की निर्भरता इस हद तक बढ़ गयी है कि इन सुविधाओं के अभाव में मानो हमारा जीवन ही मुश्किल हो जाएगा. वर्तमान में सामान्य बातचीत, कारोबार, सरकारी कामकाज, शिक्षा, बैंकिग लेनदेन, शॉपिंग जैसी गतिविधियां ऑनलाइन याने डिजिटल माध्यम से ही फल फूल रही है. दिन प्रतिदिन आम कार्यकलापों में जिस रफ्तार से सूचना और प्रौद्योगिकी का उपयोग बढ़ रहा है, उसके चलते वर्ष 2025 तक भारत में इंटरनेट उपभोक्ताओं की संख्या 100 करोड़ तक पहुँचने का अनुमान है. एक ओर सेवा प्रदाता कंपनियां डिजिटल मध्यम से प्रदान की जाने वाली सुविधाओं में तेजी ला रही हैं. लगातार इस दिशा में निरंतर अनुसंधान हो रहे हैं कि प्रक्रियाओं को सरलतम बनाकर कारोबार को और आसान कर अपने आर्थिक लाभ में वृद्धि लायी जाए. आज के आधुनिक दौर में मनुष्य जीवन बेहतर से बेहतरीन बनाने में सूचना और प्रौद्योगिकी काफी अहम साबित हो रही है. मगर जब अद्यतन सूचना और प्रोद्योगिकी तकनीक ने सामाजिक, आर्थिक और राजनैतिक जगत मे क्रांति लायी है, तब ये अपराध जगत से अछूती कैसे रह पाती? अत: जब असामाजिक तत्वों द्वारा कुकर्मों में सूचना और प्रोद्योगिकी का प्रयोग होता है तो उसे साइबर अपराध कहा जाता है. आज कल कंप्यूटर हमारे अस्तित्व का एक अनिवार्य हिस्सा बन गए हैं, इसी वजह से उन्होंने साइबर–अपराध के लिए अनुकूल वातावरण भी विकसित किया है. तेजी से बदलते परिवेश और आईटी उद्योग के महत्वपूर्ण योगदान के मद्देनजर साइबर अपराध एक बड़ी चुनौती है. साइबर अपराध आम तौर पर उन अपराधियों द्वारा किया जाता है जिनके पास तकनीकी कौशल होता है जो कंप्यूटर तक पहुंच हासिल करने और अपराध करने के लिए कानून से एक कदम आगे सोच सकते हैं. आज विश्व का हर देश साइबर अपराधों से निपटने के लिए प्रयत्नशील है. संचार प्रणाली में 'वर्ल्ड वाइड वेब' को रीढ़ की हड्डी माना जाता है और उस पर असामाजिक तत्वों के बुरी नजर पड़ी है और 'वर्ल्ड वाइड वेब' का प्रयोग साइबर अपराधों को अंजाम देने के लिए किया जा रहा है. इस कारण साइबर अपराध के बारे में जागरूकता लाना प्रत्येक नागरिक की जिम्मेदारी है.

राष्ट्रीय साइबर सुरक्षा समन्वयक एम यू नायर ने 'सिनर्जिया कॉन्क्लेव 2023' में एक सत्र को संबोधित करते हुए कहा कि भारतीय साइबरस्पेस में पिछले छह महीनों के दौरान औसतन 2127 बार साइबर घटनाएं सामने आई हैं, जो वैश्विक औसत 1108 से कहीं अधिक है. उनका कहना है कि साइबरस्पेस पर विघटनकारी प्रेक्टिस को रोकने और सीमित करने के लिए सभी देशों को एकजुट होने का समय आ गया है. साइबर सुरक्षा के आँकड़े बताते हैं कि प्रति दिन 2,200 साइबर हमले होते हैं, औसतन हर 39 सेकंड में एक साइबर हमला होता है. अमेरिका में, डेटा उल्लंघन की लागत औसतन

9.44मिलियन $ है, और साइबर अपराध की लागत 2023 तक 8 ट्रिलियन $ होने का अनुमान है. हर दिन 300,000 नए गैलवेयर बनाए जाते हैं, जिनमें से 92% ईमेल के माध्यम से वितरित किए जाते हैं और उनकी पहचान अवधि 49 दिनों की होती है. स्टेटिस्टा ने खुलासा किया है कि सेवा के रूप में वैश्विक सुरक्षा (एसईसीएएएस) बाजार 2026 में 22 अरब डॉलर से अधिक तक पहुंचने का अनुमान है. अत: हमारे संगठनों के लिए खुद को पूरी तरह से सुरक्षित रखना मुश्किल है.

'अर्थव्यवस्था' देश के विकास और प्रगति के लिए निर्धारक नीव है इसीलिए बैंकिग क्षेत्र को अर्थव्यवस्था की रीढ़ माना जाता है. नरसिम्हा समिति (1991–1998) जो वित्तीय मामलों पर सिफारिश के लिए थी, ने सुझाव दिया कि आईटी का उपयोग बैंकिग क्षेत्र में भी किया जाना चाहिए ताकि इसे कामकाज को और अधिक कुशल बनाया जा सके. उन सिफ़ारिशों के अनुसार भारत मे सूचना और प्रौद्योगिकी तकनीकी के बढ़ते प्रभावों की वजह से हम अपनी दैनिक बैंकिग गतिविधियां बड़ी आसानी से कर लेते हैं. जैसे ऑनलाइन बैंकिग और क्रेडिट कार्ड सेवाएँ, डेबिट कार्ड से ऑनलाइन भुगतान ग्राहक दिन के 24 घंटे सभी प्रकार की बैंक सुविधाओं का उपयोग कर सकते हैं और वे इंटरनेट और सेल फोन का उपयोग करके दुनिया में कहीं से भी आसानी से लेनदेन कर सकते हैं, अपने खाते चला सकते हैं. सभी जानते हैं, ये सेवाएँ ग्राहकों के लिए उपयोगी हैं, लेकिन इनका एक विपरीत पक्ष भी है, जिसमें हैकर्स और डकैतियाँ शामिल हैं. वे बैंकिंग वेबसाइटों और ग्राहकों के खातों में सेंध लगाकर उन सेवाओं का लाभ उठाते हैं, जिससे खातों में गड़बड़ी होती है और ग्राहकों के खातों से पैसों की चोरी होती है. जबकि बैंकिग क्षेत्र ने अपनी सेवाओं का विस्तार किया है और नवाचार के माध्यम से उत्कृष्ट ग्राहक सेवा प्रदान करने का लक्ष्य रखा है, साइबर अपराध एक समस्या बनी हुई है. साइबर अपराधी इंटरनेट पर आसानी से संपर्क कर सकते हैं. साइबर–अपराध बड़े पैमाने पर मौद्रिक और गैर मौद्रिक नुकसान का कारण बनता है, जिसका खामियाजा न केवल ग्राहकों को उठाना पड़ता है, बल्कि बैंकों को भी उठाना पड़ता है, जिससे देश की अर्थव्यवस्था प्रभावित होती है. जब वायरस उत्पन्न होते हैं और अन्य उपकरणों पर फैलते हैं, या जब संवेदनशील व्यावसायिक जानकारी इंटरनेट पर पोस्ट की जाती है, तो उसे गैर–मौद्रिक साइबर अपराध कहा जाता है. फ़िशिंग और फ़ार्मिंग सबसे लोकप्रिय उदाहरण हैं. इंटरनेट, एटीएम और मोबाइल बैंकिग जैसे वैकल्पिक प्लेटफार्मों के माध्यम से बढ़ी हुई ऑनलाइन पहचान के कारण, भारत में डेबिट/क्रेडिट कार्ड की मात्रा में वृद्धि देखी गई है. भविष्य में आने वाली महाक्रांति के युग में प्रवेश करने के साथ ही यह राशि और भी गति पकड़ लेगी। इस परिप्रेक्ष्य मे बैंकिग क्षेत्र के लिए साइबर खतरों के बारे में चिंताओं की जांच करना समय की मांग है. यह इस बात पर ध्यान केंद्रित करता है कि वित्तीय संस्थान साइबर–अपराध की घटनाओं से निपटने के लिए कितने सुसज्जित हैं.

साइबर अपराध के प्रभाव –

साइबर अपराध का लोगों पर दीर्घकालिक परिणाम हो सकता है. साइबर हमलावर ऋण लेने, क्रेडिट हड़पने, हैकिग आदि जैसे साइबर खतरों को अंजाम देते हैं, जिसका बैंकिग व्यवसाय पर विनाशकारी प्रभाव हो सकता है. **वित्तीय क्षति, गोपनीय जानकारी का उल्लंघन, कानूनी परिणाम, पहचान योग्य जानकारी में तोड़फोड़ और चोरी, प्रतिष्ठा जोखिमों के संपर्क में परिचालन जोखिम आदि.**

साइबर अपराध के कारण –

1. डेटा तक आसान पहुंच: एक बार जब कोई साइबर हमलावर कंप्यूटर सिस्टम में पहुंच प्राप्त करने में सक्षम हो जाता है, तो उनके पास ग्राहकों के निजी वित्तीय दस्तावेजों सहित व्यक्तिगत डेटा तक पहुंच हो सकती है, जिसे कॉपी किया जा सकता है या एक छोटे हटाने योग्य डिवाइस में स्थानांतरित किया जा सकता है. चूंकि सूचना प्रौद्योगिकी बैंकों, व्यक्तियों, निगमों, सरकारी एजेंसियों आदि के संचालन को शक्ति प्रदान करती है, इसलिए उनके कंप्यूटर पर संसाधित गोपनीय डेटा और जानकारी का असुरक्षित भंडारण एक गंभीर खतरा पैदा करता है.

2. उपयोगकर्ता की लापरवाही: कंप्यूटर सिस्टम का उपयोग करने वाले सभी अधिकारियों को कंप्यूटर में संग्रहित अपने गोपनीय डेटा और जानकारी की सुरक्षा के लिए बहुत सावधान और सतर्क रहना चाहिए। पासवर्ड और व्यक्तिगत पहचान संख्या (पिन) के उचित उपयोग के माध्यम से वे पहुंच को सीमित कर सकते हैं. उनकी ओर से कोई भी लापरवाही साइबर अपराधियों को कुछ उपकरणों और रिकॉर्ड तक आसान पहुंच प्रदान करेगी.

3. संगठनों और बैंकों में आंतरिक नियंत्रण का अभाव: बैंक अपनी दैनिक गतिविधियों के लिए विभिन्न प्रकार के ऑपरेटिंग सिस्टम का उपयोग करते हैं; इसलिए बैंकों को यह सुनिश्चित करना चाहिए कि उनके पास चालू आंतरिक नियंत्रण और आईटी ऑडिट प्रणालियाँ हैं, अन्यथा अकुशल सॉफ्टवेयर और हार्डवेयर प्रणालियों के कारण कम्प्यूटरीकृत वातावरण में चूक हो सकती है.

बैंकिंग क्षेत्र से जुड़े साइबर अपराध के प्रकार–

1. हैकिंग: हैकिंग एक साइबर अपराध है जिसमें एक व्यक्ति किसी सिस्टम तक अवैध पहुंच प्राप्त करता है या ग्राहकों के खातों या

बैंकिंग साइटों को हैक करके सुरक्षा तंत्र को चकमा देने का प्रयास करता है. हैकिंग का अपराध साबित होने पर दोषी को आईटी अधिनियम के तहत तीन साल की जेल या पांच लाख रुपये तक का जुर्माना या दोनों की सजा हो सकती है.

2. कुंजी लॉगिंग: इसे कीस्ट्रोक लॉगिंग या कीबोर्ड कैप्चरिंग कहा जाता है. यह कीबोर्ड पर दबाई गई कुंजी को गुप्त रूप से रिकॉर्ड करने (लॉगिंग) करने की प्रक्रिया है ताकि इसका उपयोग करने वाला व्यक्ति इस बात से बेखबर रहे कि उनकी गतिविधियों पर नज़र रखी जा रही है और ये बैंकिंग विवरण आदि जैसी गोपनीय जानकारी चुराने के लिए अविश्वसनीय रूप से हानिकारक हैं.

3. वायरस: यह एक प्रकार का स्व–प्रतिकृति प्रोग्राम है जो स्वयं की प्रतियां डालकर निष्पादन योग्य कोड या दस्तावेज़ों को संक्रमित करता है उसके पश्चात फ़ाइल को असामान्य रूप से व्यवहार करने का कारण बनता है. यह प्रोग्राम फ़ाइलों और ऑपरेटिंग सिस्टम जैसी निष्पादन योग्य फ़ाइलों से जुड़कर फैलता है. निष्पादन योग्य फ़ाइल को लोड करने से वायरस की नई प्रतियां बन सकती हैं.

4. वर्म्स: ऐसे प्रोग्राम हैं जो स्वयं की प्रतिकृति बना सकते हैं और पीड़ित के कंप्यूटर से अन्य कंप्यूटरों को प्रतियां भेज सकते हैं. वर्म किसी फ़ाइल को बदलते या हटाते नहीं हैं; इसके बजाय, वे उपयोगकर्ता के कंप्यूटर से अन्य कंप्यूटरों को गुणा और प्रतियां भेजते हैं.

5. स्पाइवेयर: स्पाइवेयर ऑनलाइन बैंकिंग क्रेडेंशियल्स चुराने और धोखाधड़ी के उद्देश्यों के लिए उनका उपयोग करने का सबसे आम तरीका है. स्पाइवेयर कंप्यूटर और वेबसाइटों के बीच जानकारी एकत्र या प्रसारित करके संचालित होता है. यह अधिकतर सॉफ़्टवेयर डाउनलोड करने के लिए फर्जी 'पॉप अप' विज्ञापनों द्वारा स्थापित किया जाता है. उद्योग मानक एंटीवायरस उत्पाद इस प्रकार के सॉफ़्टवेयर का पता लगाते हैं और उन्हें हटा देते हैं.

6. फ़िशिंग: फ़िशिंग एक प्रकार की धोखाधड़ी है जिसमें निजी जानकारी जैसे डेबिट/क्रेडिट कार्ड नंबर, ग्राहक आईडी, आईपिन, सीवीवी नंबर, कार्ड समाप्ति तिथि इत्यादि ईमेल के माध्यम से चुरा ली जाती है जो वास्तविक स्रोत से आती है. फ़िशिंग त्वरित संदेश और **ईमेल स्पूफ़िंग** के उपयोग के माध्यम से की जाती है. इस प्रकार के अपराध में, धोखाधडी करने वाले बैंक के अधिकारियों की तरह कार्य करते हैं और वे एक सीधा लिंक बनाते हैं जो लक्षित ग्राहकों को एक नकली पृष्ठ पर ले जाता है जो वास्तविक बैंक वेबसाइट के समान दिखता है. फिर अर्जित गोपनीय जानकारी का उपयोग ग्राहक के खाते पर धोखाधड़ीपूर्ण लेनदेन करने के लिए किया जाता है. फ़िशर आजकल ऐसे अपराध करने के लिए **एसएमएस (स्मिशिंग)** और **मोबाइल (वॉयस फ़िशिंग)** का भी उपयोग करते हैं.

7. फार्मिंग: फार्मिंग इंटरनेट के माध्यम से की जाती है. जब कोई ग्राहक किसी बैंक की वेबसाइट पर लॉग इन करता है, तो हमलावर यूआरएल को इस तरह से हाईजैक कर लेते हैं कि वे दूसरी वेबसाइट पर पहुंच जाते हैं, जो झूठी होती है लेकिन बैंक की मूल वेबसाइट की तरह दिखाई देती है.

8. एटीएम स्किमिंग और प्वाइंट ऑफ सेल अपराध: वास्तविक कीपैड के रूप में दिखने के लिए मशीन कीपैड के ऊपर एक स्किमिंग डिवाइस स्थापित करना या मशीन के एक हिस्से के रूप में दिखने के लिए कार्ड रीडर पर चिपकाए जाने वाला उपकरण एटीएम मशीनों या पीओएस सिस्टम सुरक्षा मे सेंध करने की एक रणनीति है. इन उपकरणों पर मैलवेयर भी इंस्टॉल किया जा सकता है जो सीधे क्रेडिट कार्ड डेटा चुराता है. एटीएम मशीनों में सफलतापूर्वक स्थापित किए गए स्कीमर व्यक्तिगत पहचान संख्या (पिन) कोड और कार्ड नंबर प्राप्त करते हैं, जिन्हें फिर धोखाधड़ी वाले लेनदेन करने के लिए कॉपी किया जाता है.

9. डीएनएस कैश पॉइज़निंग : डीएनएस सर्वर का उपयोग किसी कंपनी के नेटवर्क में पहले प्राप्त क्वेरी परिणामों को कैशिंग करके रिज़ॉल्यूशन प्रतिक्रिया समय बढ़ाने के लिए किया जाता है. डीएनएस सॉफ्टवेयर में खामी का फायदा उठाकर डीएनएस सर्वर पर साइबर हमले किए जाते हैं. बैंक ग्राहकों को अपराधियों द्वारा नियंत्रित सर्वर पर भेजा जा सकता है, जिसका उपयोग मैलवेयर परोसने के लिए किया जा सकता है या बैंक ग्राहकों को किसी वैध वेबसाइट की नकली जानकारी प्रदान करने के लिए धोखा दिया जा सकता है. एक हमलावर आईपी एड्रैस को स्पूफ करके ग्राहकों को हाईजैक कर सकता है; जैसे किसी दिए गए डीएनएस सर्वर पर किसी बैंक की वेबसाइट के लिए डीएनएस प्रविष्टियाँ और उन्हें उनके द्वारा नियंत्रित सर्वर के आईपी पते से बदलना.

10. मैलवेयर आधारित हमले: इलेक्ट्रॉनिक बैंकिंग सेवाओं के लिए सबसे खतरनाक साइबर खतरों में से एक मैलवेयर–आधारित हमले हैं. ऐसे हमलों में एक दुर्भावनापूर्ण कोड बनाया जाता है. इन दिनों बैंकिंग उद्योग में मैलवेयर हमलों की संख्या

बढ़ रही है. ज़ीउस, स्पाईआई, कार्बेप, किन्स और टिनबा ये कुछ सबसे प्रसिद्ध बैंकिंग मैलवेयर हैं. लगभग हर वायरस की दो विशेषताएं होती हैं: एक, यह सिस्टम में पिछले दरवाजे से प्रवेश सुनिश्चित करता है और दूसरा, यह उपयोगकर्ता की क्रेडेंशियल जानकारी चुरा लेता है.

बैंकों पर साइबर अपराध का प्रभाव –

आर्थिक उदारीकरण और वैश्विकीकरण स्थितियों के कारण, दुनिया में बैंकिंग उद्योग एक कठिन स्थिति का सामना कर रहा है. जोखिमों का बेहतर विश्लेषण करने और उन्हें कम करने के लिए, बैंकिंग उद्योग को अपनी मौजूदा प्रथाओं की समीक्षा करने के लिए मजबूर किया जा रहा है. जोखिम प्रबंधन के लिए, प्रौद्योगिकी–संचालित दृष्टिकोण का उपयोग किया गया है. हालाँकि, प्रौद्योगिकी प्रगति ने बैंकिंग सेवाओं को सुलभ और किफायती बना दिया है, लेकिन इससे साइबर हमलों का निशाना बनने की संभावना बढ़ गई है. साइबर चोरों ने न केवल पैसे चुराने के लिए, बल्कि कंपनियों की जासूसी करने और महत्वपूर्ण व्यावसायिक जानकारी तक पहुंच हासिल करने के लिए भी तरीके विकसित किए हैं, जिसका बैंक के वित्त पर अप्रत्यक्ष प्रभाव पड़ता है. ऐसे साइबर अपराधों से निपटने के लिए, बैंकिंग उद्योग को एक मॉडल बनाने के लिए राष्ट्रीय अधिकारियों और निगरानी संगठनों के साथ काम करना चाहिए जो नियंत्रण में सहायता करेगा। बैंकिंग उद्योग में एक कुशल संकलन (डाटा बेस) की आवश्यकता है जो साइबर अपराध में पैटर्न का पता लगा सकता है और उनके आधार पर एक मॉडल विकसित कर सकता है.

भारत में साइबर हमलों के उदाहरण –

* **पुणे में कॉसमॉस बैंक** पर 2018 में हुए साइबर हमले से 94.42 करोड़ रुपये की लूट ने भारत में पूरे बैंकिंग उद्योग को हिलाकर रख दिया। हैकर्स ने बैंक के एटीएम सर्वर तक पहुंच हासिल कर ली और बड़ी संख्या में रुपए डेबिट कार्डधारकों और वीजा की निजी जानकारी चुरा ली। पैसा ख़त्म हो गया, और 28 देशों के हैकर गिरोहों ने सूचना मिलते ही धनराशि निकाल ली.

* **एटीएम सिस्टम हैक–** कैनरा बैंक के एटीएम सर्वर को 2018 में साइबर हमले के लिए निशाना बनाया गया था. कई बैंक खातों से बीस लाख रुपये साफ कर दिए गए. हैकर्स ने डेबिट कार्डधारकों से जानकारी हासिल करने के लिए स्किमिंग मशीनों का इस्तेमाल किया। चोरी की गई जानकारी से जुड़े लेन–देन की राशि रुपये से भिन्न थी. यदि डेटा के दुरुपयोग से बचने के लिए एटीएम में सुरक्षा तंत्र में सुधार किया जा सके तो इससे बचा जा सकता है.

* **आरबीआई फ़िशिंग घोटाला** – एक साहसिक फ़िशिंग प्रयास में एक फ़िशिंग ईमेल, जो कथित तौर पर आरबीआई से आया था, ने प्राप्तकर्ता को 48 घंटों के भीतर 10 लाख रुपये की पुरस्कार राशि देने का वादा किया था. यदि उन्होंने एक कनेक्शन पर क्लिक किया जो उन्हें एक ऐसी वेबसाइट पर ले गया जो बिल्कुल आरबीआई की आधिकारिक वेबसाइट की तरह दिखती थी, पूर्ण एक ही लोगो और वेब पते के साथ. उसके बाद, उपयोगकर्ता से उसका पासवर्ड, आई–पिन और बचत खाता नंबर जैसी व्यक्तिगत जानकारी का खुलासा करने के लिए कहा जाता है. दूसरी ओर, आरबीआई ने अपनी आधिकारिक वेबसाइट पर फर्जी फ़िशिंग ई–मेल के बारे में अलर्ट जारी किया.

साइबर अपराध को रोकने के तरीके –

बैंकिंग उद्योग में अपराधों में चिंताजनक रूप से वृद्धि हुई है और आर्थिक नुकसान हुआ है. बैंकिंग हमारी अर्थव्यवस्था का सबसे महत्वपूर्ण आधार है, इसलिए इसे साइबर हमलों से अवश्य रोका जाना चाहिए. बैंकों और ग्राहकों को इससे जुड़े जोखिम और साइबर हमले से निपटने के लिए सुरक्षा उपायों के बारे में जागरूक किया जाना चाहिए. साइबर सुरक्षा नीति के सभी मामलों के प्रभावी कार्यान्वयन के लिए, सरकार ने राष्ट्रीय सुरक्षा परिषद को नोडल एजेंसी बनाकर एक 'अंतर–विभागीय सूचना सुरक्षा कार्य बल (आईएसटीएफ)' की स्थापना की है. राष्ट्रीय नोडल एजेंसी 'इंडियन कंप्यूटर इमरजेंसी रिस्पॉन्स टीम (सीईआरटी–इन)' है, जिसे कंप्यूटर सुरक्षा घटनाओं के घटित होने पर उनकी जांच करने का काम सौंपा गया है. साइबर अपराध से जुड़ी मुख्य समस्या क्षेत्राधिकार की है. साइबर अपराध हर राज्य में होता है, इसलिए कोई भी व्यक्ति, चाहे वह कहीं भी रहता हो, साइबर अपराधों को पहचानने और निगरानी करने में सक्षम होना चाहिए. कुछ मामलों में, साइबर अपराध के पीड़ित कई कारणों से साइबर अपराध की रिपोर्ट करने में असमर्थ हो सकते हैं, जैसे दूर के इलाके में रहना, यह अनिश्चित होना कि कहां रिपोर्ट करें और गोपनीयता संबंधी चिंताएँ. एक केंद्रीकृत ऑनलाइन साइबर अपराध निगरानी प्रणाली के अभाव के परिणामस्वरूप, कई साइबर अपराध की घटनाएं दर्ज नहीं की जाती हैं. आईटी अधिनियम को संशोधित किया जाना चाहिए ताकि साइबर अपराध की परिभाषा के साथ–साथ उन उदाहरणों की सूची भी शामिल की जा सके जिनमें अधिनियम में अलौकिक अधिकार होंगे. भारत में साइबर विनियमन के लिए विधायी आधार को शामिल करने के लिए आईटी अधिनियम के दायरे का विस्तार किया जाना चाहिए. प्रत्येक कर्मचारी के पास अपना स्वयं का

उपयोगकर्ता खाता होना चाहिए, नीति के अनुसार हर तीन महीने में पासवर्ड बदलना आवश्यक है. कर्मचारियों को अनधिकृत सॉफ़्टवेयर डाउनलोड या इंस्टॉल करने की अनुमति नहीं दी जानी चाहिए. सभी कर्मचारियों को अज्ञात स्रोतों से ईमेल अटैचमेंट खोलने या अपलोड करने के खतरों के बारे में सूचित किया जाना चाहिए। संस्थान के बारे में संवेदनशील जानकारी लीक या साझा न करने के महत्व के बारे में कर्मियों को शिक्षित करें. बैंक के आईटी विभाग को यह सुनिश्चित करना चाहिए कि संगठन में प्रत्येक कार्य केंद्र और इंटरनेट से जुड़े डिवाइस पर फ़ायरवॉल सक्षम है क्योंकि फ़ायरवॉल अनधिकृत स्रोतों से सभी संचार को अवरुद्ध करता है. बैंकों को 'दो-कारक प्रमाणीकरण (2 एफ ए)' ऐप्स या भौतिक सुरक्षा कुंजी का उपयोग करना चाहिए और जहां भी संभव हो, सभी ऑनलाइन खातों पर 2 एफ ए सक्षम करना चाहिए. विभाग यह सुनिश्चित करेगा कि सभी पीसी के ऑपरेटिंग सिस्टम को नियमित सुरक्षा अपडेट प्राप्त हों. यह पता लगाने के लिए कि नेटवर्क पर कोई रैंसमवेयर या दुर्भावनापूर्ण सॉफ़्टवेयर है या नहीं, सभी पीसी पर एंटी-स्पाइवेयर और एंटी-वायरस सॉफ़्टवेयर इंस्टॉल होना चाहिए. सभी पासवर्ड और वायरलेस नेटवर्क को सुरक्षित और अच्छी तरह से संरक्षित रखा जाना चाहिए. बैंकों को डायनेमिक डिवाइस प्रमाणीकरण और वेब-आधारित लेनदेन सत्यापन जैसे सत्यापन तरीकों को नियोजित करना चाहिए क्योंकि अधिकतर उपभोक्ता मोबाइल उपकरणों का उपयोग करते हैं. ग्राहकों को अपने लेनदेन की वैधता की पुष्टि करने वाले बैंकों से सूचनाएं और स्वचालित संदेश प्राप्त होने चाहिए. ग्राहकों को यह निर्देश दिया जाना चाहिए कि व्यक्तिगत खातों की जानकारी मांगने वाले किसी भी स्रोत की वैधता को कैसे सत्यापित किया जाए. ग्राहकों को बैंक की वेबसाइटों का उपयोग करते समय सुरक्षित रहने के निर्देश भी दिए जाने चाहिए. बैंकिग एप्लिकेशन या इंटरनेट बैंकिग का उपयोग करते समय, सुरक्षित नेटवर्क का उपयोग करें. ऑनलाइन लेनदेन की अत्यधिक आसानी, लागत बचत और गति के कारण, भारतीय उपभोक्ता तेजी सै ऑनलाइन सेवाओं को पसंद कर रहे हैं. इसके अलावा, वित्तीय संस्थान कम परिचालन लागत के कारण कैशलेस लेनदेन की संख्या बढ़ाने की उम्मीद में उपभोक्ताओं को रोमांचक सौदे पेश कर रहे हैं. ऐसा कहा जा रहा है कि, यह संकेत दिया जा सकता है कि साइबर अपराध से निपटने के लिए आर्थिक संस्थानों की साइबर सुरक्षा पहल एक गतिशील तकनीकी वातावरण और बढ़ते हमलावर कौशल से आगे निकल रही है.

संक्षेप मे आज हमारे देश का शीर्ष नेतृत्व और सारी यंत्रणा देश को 21वी सदी का शक्तिशाली विकसित डिजिटल भारत बनाने में प्रयासरत है और दूसरी ओर आए दिन साइबर धोखाधड़ी की घटनाएँ तेजी से रफ्तार पर है. हमारा देश **'वसुधैव कुटुंबकम्'** की महान भावना से सारे विश्व को मानव कल्याण के लिए एकजुट कर रहा है और दूसरी ओर साइबर अपराध भी अपना जाल फैला रहा है. समाज में दिन प्रतिदिन अपराध बढ़ते ही जा रहे हैं. मुख्य कारण हमारी बदलती जीवनशैली, सामाजिक परिस्थितियां, मानसिक तनाव, सोशल मीडिया का बढ़ता उपयोग, सस्ता इंटरनेट हैं. कई लोग इंटरनेट पर वीडियो देखकर ही अपराध करना सीखते हैं, तो कुछ सोशल मीडिया के जरिए लोगों को भड़काते हैं. एक कारण यह भी है कि अपराधियों को सजा का डर नहीं है, देश का कानून बहुत लचीला है. अपराधी इसका फायदा उठाकर छूट जाते हैं. साइबर अपराधों की तेजी के साथ निष्पक्षता से जांच के साथ साथ इन अपराधों के प्रक्षेपवक्र का व्यावहारिकता से अध्ययन करके उन्हे रोकने की प्रक्रिया बनाने के लिए पर्याप्त कदम उठाने की आवश्यकता है. सख्त कानून, सोशल मीडिया पर नियंत्रण, बच्चों की सही परवरिश, हमारे नैतिक कर्तव्य के प्रति जिम्मेवारी भी बहुत कारगर साबीत होंगी. अपराधिक प्रवृत्ति को कम करने के लिए केवल कानून व्यवस्था ही जिम्मेदार नहीं है. हमारा भी कुछ नैतिक और सामाजिक दायित्व बनता है. यदि आप अपने आसपास किसी को ऐसे अपराधिक बातें करते हुए सुनें या देखें तो उसका विरोध करें. सोशल मीडिया अपराध का कारण बन रहा है तो यही उसे रोकने का हथियार भी बन सकता हैं. ऐसे अपराधियों के बारे में सोशल मीडिया पर डालना चाहिए. ताकि अपमान के डर से लोग ऐसे अपराध करने से बचें. इस परिवेश मे जहां तक हो सके आपराधिक तत्वों से खुद भी बचें और दूसरों कों भी बचाए. किसी विद्वान ने सही कहा है –

''बहुनिष्कपटद्रोही बहुधान्योपधातक: .
रन्धान्वेषी च सर्वत्र दूषको मूषको यथा ..''

अर्थात चूहे की तरह दुष्ट भी निष्कपटी लोगों का द्रोह करनेवाला (कीमती वस्त्र को खा जाने वाला), ज्यादा करके दूसरे का घात करनेवाला (धान्य का नाश करनेवाला) और छिद्र ढूंढनेवाला (दर को ढूँढने वाला) होता है.

अतः वर्तमान परिस्थितियों में बैंकिंग मे साइबर अपराध से बचने का मूलमंत्र कुछ इसप्रकार है –

''जानकारी ही हथियार है और बचाव ही उपाय है''

मुकेश अशोक सूर्यवंशी
प्रबंधक
बैंक ऑफ बड़ौदा

राजभाषा में एआई (कृत्रिम बुद्धिमत्ता)

मनुज की बातें और मस्तिष्क
मशीनें खुद बन जाएंगी

गणित से आगे जाकर के
कहानी ये लिख आएंगी

सभी भाषा की बातों को
मशीनें अब समझाएंगी

राज न रह पाए कुछ भी
एआई सब कह जाएगी

भाषा

भाषा आम तौर पर संचार की एक प्रणाली को संदर्भित करती है जिसमें मनुष्य द्वारा विचारों, भावनाओं और सूचनाओं को व्यक्त करने के लिए ध्वनियों, शब्दों और व्याकरण का उपयोग किया जाता है. भाषा के दो मुख्य प्रकार हैं:

1. **प्राकृतिक भाषा:** यह वह भाषा है जिसका उपयोग मनुष्य रोजमर्रा के संचार के लिए करते हैं, जैसे कि अंग्रेजी, स्पेनिश, चीनी आदि। प्राकृतिक भाषाएँ व्याकरण के नियमों, शब्दावली और मुहावरों के साथ विविध और जटिल हैं.

2. **प्रोग्रामिंग भाषा:** कंप्यूटर विज्ञान के संदर्भ में, प्रोग्रामिंग भाषा एक औपचारिक प्रणाली है जिसका उपयोग कंप्यूटर को निर्देश देने के लिए किया जाता है. उदाहरणों में पायथन, जावा, सी++ और कई अन्य शामिल हैं. ये भाषाएँ एल्गोरिदम और प्रोग्राम लिखने के लिए एक विशिष्ट वाक्यविन्यास और शब्दार्थ का उपयोग करती हैं.

भाषा मानव संस्कृति और अनुभूति का एक महत्वपूर्ण पहलू है, जो हमें ज्ञान साझा करने, विचार व्यक्त करने और जटिल सामाजिक संपर्क में शामिल होने की अनुमति देती है. यह मानव संचार का एक मूलभूत हिस्सा है और हमारे जीवन के विभिन्न पहलुओं में केंद्रीय भूमिका निभाता है.

राजभाषा

आधिकारिक भाषा वह भाषा होती है जिसे किसी विशेष देश, राज्य या अन्य अधिकार क्षेत्र में विशेष दर्जा दिया जाता है. यह पदनाम अक्सर कानूनी और सरकारी समर्थन के साथ आता है, जो दर्शाता है कि निर्दिष्ट भाषा को आधिकारिक सरकारी दस्तावेजों, कार्यवाही और सार्वजनिक संस्थानों में संचार के प्राथमिक साधन के रूप में मान्यता प्राप्त है. आधिकारिक भाषा की स्थिति का अर्थ यह भी हो सकता है कि सरकारी सेवाएं, शिक्षा और जनता के साथ संचार मुख्य रूप से उसी भाषा में संचालित किया जाता है.

अनेक भाषाई समुदायों वाले देश या क्षेत्र अपने नागरिकों के बीच एकता और प्रभावी संचार को बढ़ावा देने के लिए एक या अधिक आधिकारिक भाषाओं को नामित कर सकते हैं. कुछ मामलों में, एक ही आधिकारिक भाषा हो सकती है, जबकि अन्य में, महत्व या उपयोग की अलग-अलग डिग्री के साथ कई आधिकारिक भाषाएं हो सकती हैं.

उदाहरण के लिए:

- **संयुक्त राज्य अमेरिका:** अमेरिका में संघीय स्तर पर कोई आधिकारिक भाषा नहीं है, लेकिन अंग्रेजी सरकारी और आधिकारिक उद्देश्यों के लिए उपयोग की जाने वाली वास्तविक भाषा है.
- **भारत:** भारत का संविधान राष्ट्रीय स्तर पर हिंदी और अंग्रेजी को आधिकारिक भाषाओं के रूप में मान्यता देता है, साथ ही अलग-अलग राज्यों को अपनी आधिकारिक भाषाओं को नामित करने की स्वतंत्रता है.
- **कनाडा:** कनाडा आधिकारिक तौर पर द्विभाषी है, संघीय स्तर पर अंग्रेजी और फ्रेंच को आधिकारिक भाषाओं के रूप में मान्यता दी गई है. कुछ प्रांतों की अपनी आधिकारिक भाषाएँ भी हो सकती हैं.

आधिकारिक भाषाओं का पदनाम एक जटिल और कभी-कभी विवादास्पद मुद्दा है, खासकर विविध भाषाई समुदायों वाले क्षेत्रों में यह अक्सर ऐतिहासिक, सांस्कृतिक और राजनीतिक विचारों को प्रतिबिंबित करता है.

भारत में राजभाषा का इतिहास

भारत में आधिकारिक भाषाओं का इतिहास देश की भाषाई और सांस्कृतिक विविधता से निकटता से जुड़ा हुआ है. यहां एक संक्षिप्त अवलोकन दिया गया है:

1. स्वतंत्रता-पूर्व युग:

- ब्रिटिश शासन के दौरान, अंग्रेजी प्रशासनिक और आधिकारिक भाषा बन गई.
- हालाँकि, भारत की भाषाई विविधता का मतलब था कि लोग कई भाषाएँ और बोलियाँ बोलते थे.

2. स्वतंत्रता के बाद की अवधि (1947):

- 1947 में स्वतंत्रता प्राप्त करने पर, भारत की संविधान सभा ने भाषाई विविधता को संबोधित करने की आवश्यकता को पहचाना.
- 1950 में अपनाए गए भारत के संविधान में शुरू में राष्ट्रीय स्तर पर आधिकारिक भाषा के रूप में किसी विशेष भाषा को निर्दिष्ट नहीं किया गया था.

3. संविधान में भाषा प्रावधान:

- संविधान की आठवीं अनुसूची में शुरुआत में हिंदी और अंग्रेजी सहित 14 भाषाओं को सूचीबद्ध किया गया था.
- अनुच्छेद 343 में देवनागरी लिपि में हिंदी को भारतीय संघ की आधिकारिक भाषा घोषित किया गया, साथ ही अंग्रेजी को 15 साल की संक्रमणकालीन अवधि के लिए आधिकारिक उद्देश्यों के लिए इस्तेमाल किया जाएगा (जिसे बाद में बढ़ाया गया था).

4. राजभाषा अधिनियम 1963:

- 1963 में, राजभाषा अधिनियम लागू किया गया, जिसमें शुरुआती 15 साल की अवधि के बाद भी आधिकारिक उद्देश्यों के लिए हिंदी के साथ-साथ अंग्रेजी के उपयोग को जारी रखने का प्रावधान किया गया.
- इस अधिनियम ने राष्ट्रपति को संसद में अंग्रेजी के अलावा, आधिकारिक उद्देश्यों के लिए हिंदी के उपयोग को अधिकृत करने की अनुमति दी.

5. भाषा विवाद:

- भाषा के मुद्दे पर महत्वपूर्ण बहस और विरोध प्रदर्शन हुए, खासकर दक्षिण भारत में जहां तमिल, तेलुगु और कन्नड़ जैसी भाषाएं व्यापक रूप से बोली जाती थीं.
- विरोध के परिणामस्वरूप, सरकार ने क्षेत्रीय भाषाओं के विकास और भाषाई समानता को बढ़ावा देने के लिए कदम उठाए.

6. त्रिभाषा सूत्र:

- सरकार ने शिक्षा में त्रि-भाषा फॉर्मूला अपनाया, हिंदी भाषी राज्यों में हिंदी, अंग्रेजी और क्षेत्रीय भाषा और गैर-हिंदी भाषी राज्यों में हिंदी, अंग्रेजी और एक आधुनिक भारतीय भाषा के अध्ययन को बढ़ावा दिया.

7. संशोधन और परिवर्तन:

- पिछले कुछ वर्षों में आठवीं अनुसूची में अधिक भाषाओं को शामिल करने के लिए अनुसूचित भाषाओं की सूची में संशोधन होते रहे हैं.
- आधिकारिक और प्रशासनिक उद्देश्यों के लिए, विशेषकर राष्ट्रीय स्तर पर, अंग्रेजी का बड़े पैमाने पर उपयोग जारी है.

भारत की भाषा नीति भाषाई विविधता की मान्यता और संरक्षण के साथ एकीकृत भाषा की आवश्यकता को संतुलित करने के लिए विकसित हुई है. सरकार का लक्ष्य राष्ट्रीय और राज्य स्तर पर प्रशासन और संचार की व्यावहारिक आवश्यकताओं को संबोधित करते हुए बहुभाषावाद और भाषाई बहुलवाद को बढ़ावा देना है.

भारत की राजभाषा

भारत के संविधान के प्रावधानों के अनुसार हिंदी और अंग्रेजी भारत सरकार की आधिकारिक भाषाएँ हैं.

- हिंदी: देवनागरी लिपि में लिखी जाने वाली हिंदी को संविधान के अनुच्छेद 343 में भारतीय संघ की आधिकारिक भाषा के रूप में निर्दिष्ट किया गया है. हालाँकि, यह ध्यान रखना महत्वपूर्ण है कि भारत एक भाषाई विविधता वाला देश है जहाँ विभिन्न क्षेत्रों में बहुत सारी भाषाएँ बोली जाती हैं.
- अंग्रेजी: अंग्रेजी को एक सहायक आधिकारिक भाषा के रुप में भी नामित किया गया है जिसका उपयोग आधिकारिक उद्देश्यों जैसे राज्यों और केंद्र सरकार के बीच संचार और संसद में व्यवसाय के संचालन के लिए किया जाता है.

उल्लेखनीय है कि भारत एक लचीली और समायोजनकारी भाषा नीति का पालन करता है. भारत में राज्य और केंद्र शासित प्रदेश अपने अधिकार क्षेत्र में उपयोग के लिए अपनी आधिकारिक भाषाएं नामित करने के लिए स्वतंत्र हैं. इसके अतिरिक्त, संविधान की आठवीं अनुसूची हिंदी और अंग्रेजी सहित 22 भाषाओं को अनुसूचित भाषाओं के रूप में मान्यता देती है, और राज्य इनमें से अपनी आधिकारिक भाषाएँ निर्दिष्ट कर सकते हैं.

कृत्रिम बुद्धिमत्ता (एआई)

आर्टिफिशियल इंटेलिजेंस (एआई) उन मशीनों में मानव बुद्धि के अनुकरण को संदर्भित करता है जिन्हें मनुष्यों की तरह सोचने और सीखने के लिए प्रोग्राम किया जाता है. एआई का लक्ष्य ऐसी प्रणालियाँ और प्रौद्योगिकियाँ विकसित करना है जो ऐसे कार्य कर सकें जिनके लिए आमतौर पर मानव बुद्धि की आवश्यकता होती है, जैसे दृश्य धारणा, भाषण पहचान, निर्णय लेना और भाषा अनुवाद.

एआई के क्षेत्र में प्रमुख घटकों और तकनीकों में शामिल हैं:

1. **मशीन लर्निंग (एमएल):** एमएल एआई का एक उपसमूह है जो एल्गोरिदम के विकास पर केंद्रित है जो मशीनों को डेटा से सीखने में सक्षम बनाता है. बड़े डेटासेट पर प्रशिक्षण के माध्यम से, मशीनें उस कार्य के लिए स्पष्ट रूप से प्रोग्राम किए बिना किसी कार्य पर अपने प्रदर्शन में सुधार कर सकती है.

2. **तंत्रिका नेटवर्क:** मानव मस्तिष्क से प्रेरित, तंत्रिका नेटवर्क गहन शिक्षण का एक मूलभूत घटक है, जो मशीन लर्निंग का एक उपसमूह है. तंत्रिका नेटवर्क परतों में व्यवस्थित परस्पर जुड़े नोड्स या कृत्रिम न्यूरॉन्स से बने होते हैं. गहन शिक्षण मॉडल डेटा से जटिल पैटर्न और प्रतिनिधित्व सीख सकते हैं.

3. **प्राकृतिक भाषा प्रसंस्करण (एनएलपी):** एनएलपी में कंप्यूटर और मानव भाषा के बीच बातचीत शामिल है. यह मशीनों को मानव जैसे पाठ को समझने, व्याख्या करने और उत्पन्न करने में सक्षम बनाता है, जिससे मनुष्यों और मशीनों के बीच संचार की सुविधा मिलती है.

4. **कंप्यूटर विज़न:** कंप्यूटर विज़न मशीनों को दृश्य डेटा के आधार पर व्याख्या करने और निर्णय लेने की अनुमति देता है. इस तकनीक का उपयोग छवि और वीडियो पहचान, चेहरे की पहचान और वस्तु पहचान जैसे अनुप्रयोगों में किया जाता है.

5. **रोबोटिक्स:** एआई रोबोटिक्स के क्षेत्र में एक महत्वपूर्ण घटक है, जो रोबोटों को अपने वातावरण को समझने, निर्णय लेने और स्वायत्त रूप से कार्य करने में सक्षम बनाता है.

6. **विशेषज्ञ प्रणालियाँ:** विशेषज्ञ प्रणालियाँ किसी विशिष्ट क्षेत्र में मानव विशेषज्ञ की निर्णय लेने की क्षमता की नकल करने के लिए ज्ञान आधार और अनुमान इंजन का उपयोग करती हैं. वे ज्ञान और नियमों के माध्यम से तर्क करके जटिल समस्याओं को हल करने के लिए डिज़ाइन किए गए हैं.

7. **सुदृढ़ीकरण सीखना:** सुदृढीकरण सीखने में, मशीनें पर्यावरण के साथ बातचीत करके और पुरस्कार या दंड के रूप में प्रतिक्रिया प्राप्त करके सीखती हैं. क्रमिक निर्णय लेने के लिए इस दृष्टिकोण का उपयोग अक्सर प्रशिक्षण प्रणालियों में किया जाता है.

एआई को स्वास्थ्य देखभाल, वित्त, परिवहन और मनोरंजन सहित विभिन्न उद्योगों में लागू किया जाता है. जबकि एआई ने जबरदस्त प्रगति दिखाई है, नैतिक विचार, पारदर्शिता और एआई प्रौद्योगिकियों का जिम्मेदार उपयोग महत्वपूर्ण पहलू हैं जिन पर सकारात्मक सामाजिक प्रभाव सुनिश्चित करने के लिए सावधानीपूर्वक ध्यान देने की आवश्यकता है.

राजभाषा में आर्टिफिशियल इंटेलिजेंस

किसी सरकारी या संगठनात्मक व्यवस्था में राजभाषा के संदर्भ में कृत्रिम बुद्धिमत्ता (एआई) की भूमिका निम्न प्रकार से हो सकती है:

1. **भाषा अनुवाद सेवाएँ:** एआई–संचालित भाषा अनुवाद सेवाओं को दस्तावेज़ों, भाषणों या अन्य आधिकारिक संचारों का त्वरित और सटीक अनुवाद करने के लिए नियोजित किया जा सकता है. इससे विभिन्न आधिकारिक भाषाओं का उपयोग करने वाली संस्थाओं के बीच संचार की सुविधा मिल सकती है.

2. **प्राकृतिक भाषा प्रसंस्करण (एनएलपी):** एनएलपी एआई की एक शाखा है जो कंप्यूटर और मानव भाषाओं के बीच बातचीत पर केंद्रित है. इसका उपयोग बड़ी मात्रा में पाठ्य डेटा का विश्लेषण और समझने के लिए किया जा सकता है, जिससे भावना विश्लेषण, सूचना निष्कर्षण और सारांशीकरण जैसे कार्यों में मदद मिलती है.

3. **चैटबॉट :** नागरिकों को कई भाषाओं में जानकारी प्रदान करने और प्रश्नों का उत्तर देने के लिए एआई–संचालित चैटबॉट लागू किए जा सकते हैं. इससे ग्राहक सेवा और सार्वजनिक संपर्क की दक्षता बढ़ सकती है.

4. **भाषा–आधारित विश्लेषण:** एआई उपकरण सार्थक अंतर्दृष्टि निकालने के लिए बड़ी मात्रा में टेक्स्ट डेटा का विश्लेषण कर सकते हैं. आधिकारिक भाषाओं के संदर्भ में, इसमें सार्वजनिक भावनाओं का विश्लेषण करना, मुद्दों पर नज़र रखना या सरकारी नीतियों से संबंधित चर्चाओं के रुझान को समझना शामिल हो सकता है.

5. **वाक् पहचान:** एआई–संचालित वाक पहचान तकनीक का उपयोग बोले गए शब्दों को पाठ में बदलने के लिए किया जा सकता है. यह आधिकारिक भाषणों, साक्षात्कारों या बैठकों को रिकॉर्ड करने में उपयोगी हो सकता है, और श्रवण बाधित व्यक्तियों के लिए सामग्री को सुलभ बनाने में भी सहायता कर सकता है.

6. **भाषा संसाधन प्रबंधन:** एआई भाषा संसाधनों, जैसे शब्दकोश, शब्दावलियाँ और भाषा डेटाबेस के प्रबंधन में सहायता कर सकता है. यह आधिकारिक दस्तावेजों में भाषा के उपयोग में निरंतरता बनाए रखने में मदद कर सकता है.

7. **दस्तावेज़ सारांश:** एआई एल्गोरिदम को लंबे दस्तावेज़ों को स्वचालित रूप से सारांशित करने के लिए लागू किया जा सकता है, जिससे अधिकारियों और जनता के लिए आधिकारिक संचार के प्रमुख बिंदुओं को समझना आसान हो जाता है.

8. **अभिगम्यता विशेषताएं:** एआई प्रौद्योगिकियां आधिकारिक संचार को अधिक सुलभ बनाने में योगदान दे सकती हैं. उदाहरण के लिए, एआई–संचालित टूल का उपयोग लाइव इवेंट या मीटिंग के दौरान वास्तविक समय में भाषा अनुवाद के लिए किया जा सकता है, जिससे विविध दर्शकों के लिए समावेशिता सुनिश्चित होती है.

यह ध्यान रखना महत्वपूर्ण है कि आधिकारिक भाषा सेटिंग में एआई का अनुप्रयोग नैतिक विचारों और सांस्कृतिक संवेदनशीलता के अनुरूप होना चाहिए. इसके अतिरिक्त, विभिन्न भाषाई समुदायों में निष्पक्ष और न्यायसंगत उपचार सुनिश्चित करने के लिए, एआई मॉडल में पूर्वाग्रह के मुद्दों पर विशेष रूप से भाषा–संबंधित कार्यों पर सावधानीपूर्वक ध्यान दिया जाना चाहिए.

आर्टिफिशियल इंटेलिजेंस (एआई) के माध्यम से अनुवाद

आर्टिफिशियल इंटेलिजेंस (एआई) के माध्यम से अनुवाद में एक भाषा से दूसरी भाषा में पाठ या भाषण का स्वचालित रूप से अनुवाद करने के लिए मशीन लर्निंग एल्गोरिदम और प्राकृतिक भाषा प्रसंस्करण (एनएलपी) का उपयोग करना शामिल है. एआई–आधारित अनुवाद प्रणालियाँ तेजी से परिष्कृत हो गई हैं और विभिन्न अनुप्रयोगों के लिए व्यापक रूप से उपयोग की जाती हैं. यहां बताया गया है कि एआई अनुवाद में कैसे योगदान देता है:

1. **न्यूरल मशीन ट्रांसलेशन (एनएमटी):** आधुनिक एआई अनुवाद प्रणालियाँ अक्सर न्यूरल नेटवर्क, विशेष रूप से न्यूरल मशीन ट्रांसलेशन पर निर्भर करती हैं. एनएमटी ने पारंपरिक नियम-आधारित और सांख्यिकीय मशीनी अनुवाद विधियों की तुलना में महत्वपूर्ण सुधार दिखाया है. यह मानव-समान अनुवादों को समझने और उत्पन्न करने के लिए गहन शिक्षण मॉडल का उपयोग करता है.

2. **समानांतर कॉर्पोरा पर प्रशिक्षण:** एआई अनुवाद मॉडल को बड़े समानांतर कॉर्पोरा पर प्रशिक्षित किया जाता है, जो संबंधित अनुवादों के साथ दो या दो से अधिक भाषाओं में ग्रंथों का संग्रह है. प्रशिक्षण प्रक्रिया के दौरान मॉडल एक भाषा के वाक्यांशों और वाक्यों को दूसरी भाषा के उनके समवकक्षों के साथ जोड़ना सीखते हैं.

3. **अनुक्रम-से-अनुक्रम मॉडल:** कई एआई अनुवाद मॉडल, विशेष रूप से तंत्रिका नेटवर्क पर आधारित, अनुक्रम-से-अनुक्रम वास्तुकला को अपनाते हैं. इसका मतलब यह है कि मॉडल इनपुट के रूप में एक भाषा में शब्दों का अनुक्रम लेते हैं और आउटपुट के रूप में दूसरी भाषा में शब्दों का अनुक्रम उत्पन्न करते हैं.

4. **ध्यान तंत्र:** एआई अनुवाद मॉडल में ध्यान तंत्र अनुवाद उत्पन्न करते समय सिस्टम को इनपुट टेक्स्ट के विशिष्ट भागों पर ध्यान केंद्रित करने की अनुमति देता है. यह लंबे वाक्यों या जटिल संरचनाओं को अधिक प्रभावी ढंग से संभालने में मदद करता है.

5. **सतत सीखना:** एआई अनुवाद प्रणालियाँ समय के साथ लगातार सीख सकती हैं और सुधार कर सकती हैं क्योंकि वे अधिक डेटा के संपर्क में हैं. नए समानांतर कॉर्पोरा के साथ नियमित अद्यतन और पुनः प्रशिक्षण अनुवाद मॉडल के शोधन में योगदान देता है.

6. **मल्टीमॉडल अनुवाद:** कुछ उन्नत एआई अनुवाद प्रणालियाँ कई तौर-तरीकों को संभाल सकती हैं जिसमें पाठ को वाक् में अनुवाद करना या इसके विपरीत अनुवाद करना शामिल है. यह बोली जाने वाली भाषा के अनुवाद या बोली जाने वाली सामग्री के लिए लिखित अनुवाद तैयार करने में सक्षम बनाता है.

7 **संपादन के बाद सहायता:** एआई अनुवाद उपकरण अक्सर एक सहयोगी वातावरण में उपयोग किए जाते हैं जहां मानव अनुवादक एआई सिस्टम के साथ काम करते हैं. एआई मानव अनुवादकों को सुझाव देकर या यहां तक कि प्रारंभिक ड्राफ्ट तैयार करके अनुवाद प्रक्रिया को तेज करने में सहायता कर सकता है.

8. **रीयल-टाइम अनुवाद:** एआई-संचालित अनुवाद सेवाएं विभिन्न अनुप्रयोगों, जैसे लाइव चैट, वीडियो कॉन्फ्रेंस या यहां तक कि सार्वजनिक भाषणों के दौरान भी रीयल-टाइम अनुवाद प्रदान कर सकती हैं. यह वैश्विक संचार और पहुंच को बढ़ाता है.

जबकि एआई ने अनुवाद में महत्वपूर्ण प्रगति की है, यह ध्यान रखना महत्वपूर्ण है कि संदर्भ संवेदनशीलता, मुहावरेदार अभिव्यक्ति और डोमेन-विशिष्ट शब्दावली को संभालने सहित अभी भी चुनौतियां हैं. अनुवादों में उच्चतम गुणवत्ता और सटीकता सुनिश्चित करने के लिए, विशेष रूप से महत्वपूर्ण या सूक्ष्म सामग्री के लिए, मानव अनुवादक अक्सर संपादन के बाद के चरण में शामिल होते हैं. इसके अतिरिक्त, एआई अनुवाद प्रणालियों को तैनात करते समय नैतिक विचारों, सांस्कृतिक संवेदनशीलता और गोपनीयता संबंधी चिंताओं पर ध्यान दिया जाना चाहिए.

आर्टिफिशियल इंटेलिजेंस (एआई) के माध्यम से हिंदी सीखना

आर्टिफिशियल इंटेलिजेंस (एआई) के माध्यम से हिंदी सीखने में इंटरैक्टिव और व्यक्तिगत भाषा सीखने के अनुभव प्रदान करने के लिए प्रौद्योगिकी का लाभ उठाना शामिल है. हिंदी भाषा सीखने की सुविधा के लिए एआई को कई तरीकों से लागू किया जा सकता है:

1. **एआई-संचालित भाषा ऐप:** एआई का उपयोग करने वाले भाषा सीखने वाले ऐप शिक्षार्थी की दक्षता स्तर, ताकत और कमजोरियों के आधार पर वैयक्तिकृत पाठ और अभ्यास प्रदान कर सकते हैं. ये ऐप्स व्यक्तिगत सीखने की

शैलियों को अपना सकते हैं और वास्तविक समय पर प्रतिक्रिया दे सकते हैं.

2. **वाक् पहचान:** एआई-आधारित वाक पहचान तकनीक शिक्षार्थियों को अभ्यास करने और उनके उच्चारण में सुधार करने में मदद कर सकती है. यह उनकी बोली जाने वाली हिंदी की सटीकता पर तुरंत प्रतिक्रिया प्रदान कर सकता है, जिससे उन्हें अपने बोलने के कौशल को निखारने में मदद मिलेगी.

3. **चैटबॉट:** एआई-संचालित चैटबॉट हिंदी में बातचीत का अनुकरण कर सकते हैं, जिससे शिक्षार्थियों को बातचीत के संदर्भ में अपने भाषा कौशल का अभ्यास करने की अनुमति मिलती है. ये चैटबॉट उपयोगकर्ता के इनपुट का जवाब दे सकते हैं, गलतियों को सुधार सकते हैं और स्पष्टीकरण प्रदान कर सकते हैं.

4. **अनुकूली शिक्षण प्लेटफार्म:** एआई शिक्षार्थियों की प्रगति का विश्लेषण कर सकता है, उन क्षेत्रों की पहचान कर सकता है जिनमें सुधार की आवश्यकता है, और तदनुसार पाठ योजनाओं को अनुकूलित कर सकता है. यह अनुकूली शिक्षण दृष्टिकोण सुनिश्चित करता है कि शिक्षार्थी उन क्षेत्रों पर ध्यान केंद्रित करें जहां उन्हें अधिक अभ्यास की आवश्यकता है, जिससे सीखने की प्रक्रिया अधिक कुशल हो जाती है.

5. **प्राकृतिक भाषा प्रसंस्करण (एनएलपी):** एनएलपी का उपयोग हिंदी पाठों का विश्लेषण और समझने के लिए किया जा सकता है, जिससे शिक्षार्थियों को प्रामाणिक सामग्री के साथ बातचीत करने में सक्षम बनाया जा सकता है. इसमें समझ और शब्दावली निर्माण के लिए एआई सहायता से हिंदी में लेख, किताबें या समाचार पढ़ना शामिल हो सकता है.

6. **गेमिफ़ाइड लर्निंग प्लेटफ़ॉर्म:** एआई को गेमिफ़ाइड भाषा सीखने के प्लेटफ़ॉर्म में एकीकृत किया जा सकता है, जिससे हिंदी सीखने की प्रक्रिया अधिक आकर्षक और मनोरंजक हो जाएगी। इंटरैक्टिव गेम, क्विज़ और चुनौतियाँ भाषा कौशल को मज़ेदार तरीके से सुदृढ़ कर सकती हैं.

7. **वर्चुअल ट्यूटर:** एआई-संचालित वर्चुअल ट्यूटर व्यक्तिगत मार्गदर्शन प्रदान कर सकते हैं, सवालों के जवाब दे सकते हैं और व्याकरण संबंधी अवधारणाओं को समझने में शिक्षार्थियों की सहायता कर सकते हैं. ये वर्चुअल ट्यूटर 24/7 उपलब्ध हो सकते हैं, जो शिक्षार्थियों को निरंतर सहायता प्रदान करते हैं.

8. **स्पष्टीकरण के साथ भाषा अनुवाद:** एआई व्याकरणिक संरचनाओं के स्पष्टीकरण के साथ-साथ हिंदी वाक्यांशों या रढ का त्वरित अनुवाद प्रदान करके शिक्षार्थियों की सहायता कर सकता है. इससे शिक्षार्थियों को संदर्भ के अनुसार भाषा समझने में मदद मिलती है.

9. **सांस्कृतिक और प्रासंगिक अंतर्दृष्टि:** एआई-संचालित प्लेटफॉर्म हिंदी की सांस्कृतिक बारीकियों में अंतर्दृष्टी प्रदान कर सकते हैं, जिससे शिक्षार्थियों को न केवल भाषा बल्कि उस सांस्कृतिक संदर्भ को भी समझने में मदद मिलती है जिसमें इसका उपयोग किया जाता है.

10. **प्रगति ट्रैकिंग और विश्लेषण:** एआई शिक्षार्थियों की प्रगति को ट्रैक कर सकता है, प्रदर्शन डेटा का विश्लेषण कर सकता है और सुधार के क्षेत्रों में अंतर्दृष्टि प्रदान कर सकता है. यह डेटा-संचालित दृष्टिकोण शिक्षार्थियों को लक्ष्य निर्धारित करने और हिंदी दक्षता में उनकी प्रगति को मापने में मदद करता है.

यह ध्यान रखना महत्वपूर्ण है कि हालांकि एआई भाषा सीखने के अनुभवों को बढ़ा सकता है, लेकिन यह सबसे प्रभावी तब होता है जब इसका उपयोग मानव निर्देश और अभ्यास के साथ किया जाता है. एक संतुलित दृष्टिकोण जो एआई-संचालित टूल को वास्तविक दुनिया संचार, सांस्कृतिक प्रदर्शन और मानवीय प्रतिक्रिया के साथ जोड़ता है, एक व्यापक और प्रभावी हिंदी भाषा सीखने का अनुभव प्रदान कर सकता है.

निष्कर्ष

आधिकारिक भाषाओं में आर्टिफिशियल इंटेलिजेंस (एआई) की भूमिका बहुआयामी है और सरकार और संगठनात्मक सेटिंग्स के भीतर दक्षता, पहुंच और संचार के लिए महत्वपूर्ण निहितार्थ है. एआई विभिन्न तरीकों से आधिकारिक भाषाओं के

प्रवंधन और संवर्धन में योगदान देता है:

1. अनुवाद सेवाएँ: एआई आधिकारिक दस्तावेजों, भाषणों और संचार के त्वरित और सटीक अनुवाद की सुविधा प्रदान करता है, भाषा बाधाओं को तोड़ता है और विभिन्न भाषाओं का उपयोग करने वाली संस्थाओं के बीच प्रभावी संचार को बढ़ावा देता है.

2.प्राकृतिक भाषा प्रसंस्करण (एनएलपी): एनएलपी प्रौद्योगिकियां आधिकारिक भाषाओं में बड़ी मात्रा में पाठ्य डेटा के विश्लेषण और समझ को सक्षम बनाती हैं. यह क्षमता भावना विश्लेषण, सारांशीकरण और सूचना निष्कर्षण जैसे कार्यों के लिए महत्वपूर्ण है.

3.चैटबॉट: एआई–संचालित चैटवॉट कई भाषाओं में जानकारी प्रदान करके और प्रश्नों का उत्तर देकर, कुशल और सुलभ सार्वजनिक सेवाओं को सुनिश्चित करके नागरिक जुड़ाव को बढ़ाते हैं.

4.भाषा–आधारित विश्लेषण: एआई उपकरण सार्वजनिक भावनाओं का विश्लेषण करने, मुद्दों को ट्रैक करने और सरकारी नीतियों से संबंधित चर्चाओं में रुझानों की पहचान करने में मदद करते हैं. यह निर्णय लेने और नीति निर्माण के लिए बहुमूल्य अंतर्दृष्टि प्रदान करता है.

5. वाक् पहचान: एआई–संचालित वाक् पहचान तकनीक बोले गए शब्दों को पाठ में लिखने, आधिकारिक भाषणों, साक्षात्कारों और बैठकों के दस्तावेज़ीकरण की सुविधा प्रदान करने में सहायता करती है.

दस्तावेज़ सारांशीकरण: एआई एल्गोरिदम स्वचालित रूप से लंबे आधिकारिक दस्तावेज़ों को सारांशित कर सकता है, जिससे जानकारी अधिकारियों और जनता के लिए अधिक सुलभ और सुपाच्य हो जाती है.

7.अभिगम्यता विशेषताएं: एआई लाइव इवेंट या मीटिंग के दौरान वास्तविक समय में भाषा अनुवाद प्रदान करके आधिकारिक संचार को अधिक समावेशी बनाने में योगदान देता है, यह सुनिश्चित करता है कि जानकारी विभिन्न भाषाएं बोलने वाले व्यक्तियों के लिए पहुंच योग्य है.

8.निरंतर सीखना और सुधार: एआई सिस्टम लगातार विकसित हो रही भाषाई बारीकियों को सीख और अनुकूलित कर सकता है, जो अनुवाद मॉडल और भाषा प्रसंस्करण क्षमताओं के शोधन में योगदान देता है.

इन फायदों के बावजूद, आधिकारिक भाषाओं में एआई के एकीकरण को सावधानी से करना महत्वपूर्ण है. विभिन्न भाषाई समुदायों में निष्पक्ष और न्यायसंगत उपचार सुनिश्चित करने के लिए एआई मॉडल में नैतिक विचारों, सांस्कृतिक संवेदनशीलता और संभावित पूर्वाग्रहों को संबोधित किया जाना चाहिए. इसके अलावा, एआई सिस्टम के आउटपुट को मान्य करने और बढ़ाने के लिए मानवीय निरीक्षण आवश्यक है, खासकर उन संदर्भों में जहां बारीकियां, संदर्भ और सांस्कृतिक समझ सर्वोपरि हैं.

संक्षेप में,एआई और आधिकारिक भाषाओं के बीच तालमेल प्रभावी संचार, समावेशिता और पहुंच को बढ़ावा देने की अपार संभावनाएं रखता है, जो अंततः भाषाई रूप से विविध वातावरण में सरकारों और संगठनों के कुशल कामकाज में योगदान देता है. इस एकीकरण के लाभों को अधिकतम करने के लिए एआई की क्षमताओं का लाभ उठाने और भाषा–संबंधी कार्यों में मानवीय स्पर्श को संरक्षित करने के बीच संतुलन बनाना महत्वपूर्ण है.

मुझे अभिमान मेरी मातृभाषा से
मिला सम्मान मुझको राजभाषा से

रणित चौधरी
अधिकारी
बैंक ऑफ बड़ौदा

अदावाकृत खातों का सक्रियकरण

अदावाकृत निष्क्रिय बैंक खाता की परिभाषा एवं पहचान

यदि किसी बचत या चालू खाते में दो साल से अधिक समय तक कोई लेनदेन नहीं हुआ है, तो खाता निष्क्रिय माना जाएगा. जिन खातों का उपयोग दो वर्ष से अधिक समय से नहीं किया गया है उन्हें बैंकों द्वारा नोट किया जाएगा और अलग-अलग बही-खातों में रखा जाएगा. लावारिस जमा और निष्क्रियता पर आरबीआई की अधिसूचना के अनुसार, यदि दो साल से अधिक समय तक खाते में कोई लेनदेन नहीं हुआ है तो बचत और चालू खाते को निष्क्रिय माना जाना चाहिए. किसी खाते को 'निष्क्रिय' के रूप में वर्गीकृत करने के उद्देश्य से दोनों प्रकार के लेनदेन यानी ग्राहकों के साथ-साथ तीसरे पक्ष के अनुरोध पर किए गए डेबिट और क्रेडिट लेनदेन पर विचार किया जाना चाहिए. निष्क्रिय खाता किसी बैंक या अन्य वित्तीय संस्थान में ग्राहक का खाता होता है जिसमें लंबे समय तक ब्याज जमा के संभावित अपवाद को छोड़कर कोई गतिविधि नहीं देखी गई है. हो सकता हैं कि मालिक खाते के बारे में भूल गया हो, कोई अग्रेषण पता छोड़े बिना शहर से बाहर चला गया हो, या उसकी मृत्यु हो गई हो. बहुत कम शेष राशि वाला एक निष्क्रिय खाता आसानी से लुप्त हो सकता है, और मासिक बैंक शुल्क के कारण शून्य शेष तक पहुंच सकता है जो भुगतान किए गए किसी भी ब्याज से अधिक है. यदि नहीं, तो शेष राशि राज्य को सौंप दी जाती है, जो अनुरोध पर इसे असली मालिक को वापस कर देगी. वित्तीय संस्थानों को एक निश्चित अवधि के लिए खातों के निष्क्रिय रहने के बाद निष्क्रिय खातों में रखे गए धन को राज्य के खजाने में स्थानांतरित करना आवश्यक है. समय की मात्रा राज्य के अनुसार भिन्न-भिन्न होती है.

क्या होता है जब खाता निष्क्रिय होता है?

धोखाधड़ी को कम करने के लिए बैंक कुछ समय से अपरिचालित खातों को निष्क्रिय खातों में बदल देते हैं. जब किसी खाते को निष्क्रिय के रूप में नामित किया गया है, तो आप लॉग इन नहीं कर सकते, भुगतान नहीं कर सकते, पैसे ट्रांसफर नहीं कर सकते, निकासी नहीं कर सकते, या यहां तक कि लॉग आउट भी नहीं कर सकते. जब किसी खाते को ''निष्क्रिय'' के रूप में चिन्हित किया जाता है, तो ग्राहक द्वारा प्रेरित सभी डेबिट और क्रेडिट लेनदेन अवरुद्ध हो जाएंगे. इसमें शामिल लेनदेन वित्तीय (नकद जमा/निकासी, फंड ट्रांसफर, आईएमपीएस, आरटीजीएस, एनईएफटी, या यूपीआई जैसे किसी भी लेनदेन मोड) के साथ-साथ गैर-वित्तीय (चेक बुक अनुरोध, डेबिट कार्ड अनुरोध) दोनों होंगे.

निष्क्रिय खाते को कैसे सक्रिय करें

ग्राहकों के लिए निष्क्रिय खाते को सक्रिय करने की प्रक्रिया यहां दी गई है.

चरण 1: शाखा में जाएँ और अपने हस्ताक्षर के साथ खाते में परिचालन संबंधी निर्देशों के साथ लिखित आवेदन जमा करें

चरण 2: पहचान और पते का स्व-सत्यापित प्रमाण जमा करें

चरण 3: कोई भी लेनदेन आरंभ करें और आपका खाता एक बार फिर सक्रिय हो जाएगा

अकाउंट कैसे एक्टिवेट करें

आपका बैंक को एक लिखित आवेदन जमा करना होगा. संयुक्त खातों के लिए, एकल या संयुक्त संचालन मोड के बावजूद, सभी खाताधारकों के हस्ताक्षर की आवश्यकता होगी.

आपको अपना केवाईसी (नो योर कस्टमर) दस्तावेज़ जमा करना होगा. इनमें एड्रेस प्रूफ़, पैन कार्ड और पहचान दस्तावेज शामिल होंगे.

आपको कम से कम एक वित्तीय लेनदेन करना होगा.

बैंकों को संपर्क का प्रयास

राज्य कानूनों के अनुसार वित्तीय संस्थानों को उपलब्ध नवीनतम मेल संपर्क जानकारी का उपयोग करके निष्क्रिय खातों के मालिकों से संपर्क करने का प्रयास करना आवश्यक है. यदि मालिक को खोजने का प्रयास असफल होता है, तो निष्क्रिय खातों में मौजूद संपत्ति लावारिस संपत्ति बन जाती है और उसे राज्य के राजकोष विभाग को हस्तांतरित किया जाना चाहिए.

उदाहरण के लिए, कैलिफ़ोर्निया में, चेकिंग, बचत और तब्रोकरेज खातों को निष्क्रिय होने के लिए कम से कम तीन साल तक कोई गतिविधि नहीं दिखनी चाहिए. डेलावेयर राज्य में, समान प्रकार के खातों के लिए पांच साल की निष्क्रियता अवधि होती है. सीमाओं का कानून आमतौर पर निष्क्रिय खातों पर लागू नहीं होता है, जिसका अर्थ हैं कि मालिक या लाभार्थी द्वारा भविष्य में किसी भी समय धन का दावा किया जा सकता है.

अदावाकृत निष्क्रिय खातों के लिए प्रक्रिया

लावारिस संपत्ति को बैंक में स्थानांतरित करने की कानूनी प्रक्रिया है. खाता मालिक उन संपत्तियों को पुनः प्राप्त कर सकते हैं जिन्हें निष्क्रिय समझा गया था और बैंक को हस्तांतरित कर दिया गया था. राज्यों ने क़ानून बनाए हैं जो दावा न किए गए धन को बैंक में स्थानांतरित करने की प्रक्रिया को नियंत्रित करते हैं और दावा न किए गए धन को वित्तीय संस्थानों में राशि लौटने से बचाते हैं. बैंक कानूनों के अनुसार कंपनियों को लावारिस संपत्ति को सुरक्षित रखने के लिए निष्क्रिय खातों से बैंक के सामान्य कोष में स्थानांतरित करने की आवश्यकत्ता होती है. यदि मालिक की मृत्यु हो गई हो तो बैंक रिकॉर्ड रखने और खोई हुई या भूली हुई संपत्ति को मालिकों या उनके उत्तराधिकारियों को लौटाने का काम अपने हाथ में ले लेता है.

मालिक उस बैंक में एक आवेदन दाखिल करके लावारिस संपत्ति की वसूली कर सकते हैं जिसमें खाता बिना किसी लागत या मामूली हैंडलिंग शुल्क के खोला गया था. क्योंकि बैंक लावारिस संपत्ति को हमेशा के लिए अपने पास रखता है, मालिक किसी भी समय अपनी संपत्ति पर दावा कर सकते हैं. कुछ मामलों में, स्टॉक शेयर जैसी संपत्ति बैंक द्वारा बेची जा सकती है. उस स्थिति में, शेयरों का नकद मूल्य दावेदार को भुगतान कर दिया जाता है.

संपत्ति पुनः प्राप्त करने के लिए बैंक प्रक्रियाओं के उदाहरण

लोगों को उन निष्क्रिय खातों से संपत्ति वापस पाने की अनुमति देने के लिए प्रत्येक बैंक की अपनी नीतियां और प्रक्रियाएं हैं जो बैंक को हस्तांतरित कर दी गई हैं. उदाहरण के लिए, कैलीफ़ोर्निया एक खोजने योग्य डेटाबेस रखता है जो संभावित दावेदारों को सामाजिक सुरक्षा नंबर द्वारा खोजने की अनुमति देता है. फ़्लोरिडा बैंक में एक खोज फ़ंक्शन है जिसे वह फ़्लोरिडा ट्रेजर हंट कहता है. जैसा कि शीर्षक से पता चलता है, बैंक वास्तव में लावारिस संपत्ति वापस करने के इच्छुक हैं. आखिरकार, उनके पास रिकॉर्ड रखने की ज़िम्मेदारी है लेकिन उन्हें नकदी का उपयोग करने का मौका नहीं मिलता है.

अदावाकृत निष्क्रिय खाते से अपने पैसे का दावा कैसे करें

आपका पहला कदम उस बैंक या अन्य वित्तीय संस्थान से संपर्क करना है जहां आपका खाता था. आपको उचित पहचान की आवश्यकता होगी और आपके पास कुछ सबूत होने चाहिए कि यह आपका पैसा है, जैसे बैंक विवरण.
यदि बैंक ने खाते को निष्क्रिय मान लिया है, लेकिन अभी तक केन्द्रीय बैंक (RBI) को धन हस्तांतरित नहीं किया है, तो खाते को बस पुनः सक्रिय किया जाना चाहिए.

यदि पैसा राज्य के हाथ में है, तो आपको इसे वापस पाने के लिए राज्य खजाना विभाग में जाना होगा. विभाग के पास लावारिस संपत्ति का दावा करने के लिए समर्पित एक वेबसाइट होनी चाहिए.

क्या मैं निष्क्रिय खाता बंद कर सकता हूँ?

आप निष्क्रिय खाता बंद कर सकते हैं, और आपको ऐसा करना चाहिए. ऐसा करने के लिए, वित्तीय संस्थान से संपर्क करें और उसे खाते में शेष राशि को दूसरे चालू खाते में स्थानांतरित करने के लिए कहें.

जब आप घर बदलते हैं, नौकरी बदलते हैं, या अन्यथा अपनी सामान्य दिनचर्या को बाधित करते हैं तो बैंक खाते का पता खोना आश्चर्यजनक रूप से आसान होता है.

सौभाग्य से, पैसा गायब नहीं होगा या किसी और द्वारा खर्च भी नहीं किया जाएगा। आपके बैंक के पास इन निष्क्रिय खातों को संभालने की एक प्रक्रिया है.

पैसा हमेशा के लिए आपका है. आपको बस इसका पता लगाने और दावा करने की प्रक्रिया से गुजरना होगा.

Escheatment के माध्यम से संपत्ति पुनः प्राप्त करना

निष्क्रिय बैंक खाते जैसी संपत्ति को एक निश्चित निष्क्रिय अवधि के बाद कानूनी रूप से लावारिस माना जाता है. सुप्त अवधि उस समय के बीच की अवधि है जब कोई वित्तीय संस्थान किसी खाते या संपत्ति को दावा न किए जाने की रिपोर्ट करता है और जब सरकार उस खाते या संपत्ति को त्यागने योग्य समझती है.

इस अवधि के बाद, निष्क्रिय खाते लावारिस संपत्ति बन जाते हैं. राज्यों के पास क़ानून हैं जो दावा न किए गए धन को उन वित्तीय संस्थानों में वापस जाने से बचाने की प्रक्रिया को नियंत्रित करते हैं जो उन्हें धारण करते हैं. इन कानूनों के अनुसार कंपनियों को निष्क्रिय खातों से लावारिस संपत्ति को राज्य के सामान्य कोष में स्थानांतरित करने की आवश्यकता होती है. राज्य तब रिकॉर्ड रखने और खोई या भूली हुई संपत्ति को मालिकों या उनके उत्तराधिकारियों को लौटाने की जिम्मेदारी लेता है.

मालिक बिना किसी लागत या मामूली हैंडलिंग शुल्क के राज्य के साथ एक आवेदन दाखिल करके लावारिस संपत्ति वापस पा सकते हैं. क्योंकि राज्य लावारिस संपत्ति को हमेशा के लिए अपने पास रखता हैं मालिक किसी भी समय अपनी संपत्ति पर दावा कर सकते हैं.

निष्क्रिय बैंक खाते को सक्रिय करने से पहले जानने योग्य बातें:

- बैंक खाताधारक की जोखिम श्रेणी के आधार पर ग्राहकों के निष्क्रिय बैंक खातों को नियमित कर सकता है.
- वे या तो ग्राहकों को केवाईसी दस्तावेज़ प्राप्त करने पर निष्क्रिय खातों को संचालित करने की अनुमति दे सकते हैं या आगे की सावधानी बरतने के लिए कह सकते हैं.
- बैंक विवरणों का सत्यापन भी करते हैं और दस्तावेजों के अलावा खाताधारक के हस्ताक्षर भी मांगते हैं.

खाताधारक को पता होना चाहिए कि अदावाकृत बैंक खाते का सक्रियण बिल्कुल मुफ्त है.

हाल ही में भारतीय रिजर्व बैंक ने देश भर के बैंकों को उन सभी खातों की वार्षिक समीक्षा करने का निर्देश दिया है जिनका लंबे समय से उपयोग नहीं किया गया है. बैंकों को निर्देश दिया गया है कि वे ग्राहक को 'लिखित रूप से' सूचित करें और एक वर्ष से अधिक समय तक शून्य लेनदेन के पीछे का कारण जानने का प्रयास करें. यदि ग्राहक ने अपने बैंक खाते बदल दिए हैं तो बैंक को ग्राहक तक पहुंचना होगा. नए बैंक खातों और अन्य के विवरण का उपयोग करके, निष्क्रिय खाते से पैसा स्थानांतरित किया जा सकता है. ग्राहकों को ध्यान देना चाहिए कि बचत बैंक खातों पर ब्याज समय पर जमा किया जाना चाहिए. केंद्रीय बैंक के अनुसार, यदि रकम का भुगतान नहीं किया गया है और एफडी (सावधि जमा) परिपक्व हो गई है, तो बैंक के पास लावारिस छोड़ी गई राशि पर बचत बैंक की ब्याज दर लागू होगी.

संयुक्त खाता हो तो क्या करें

ऐसा कोई खाता है जो दो लोगों के नाम पर है तो उसमें भी उपरोक्त प्रक्रिया ही अपनानी होगी. इसमें दोनों लोगों का हस्ताक्षर होना जरूरी है. यहां भी केवाईसी जमा करनी होगी. इसमें पैन, आधार या कोड और पते का सबूत हो सकता है. हालांकि, पैन कार्ड कभी भी पते का सबूत नहीं होता है.

अदावाकृत खातों पर भी मिलता है व्याज

आपका बचत खाता निष्क्रिय है और उसमें कोई भी रकम जमा है तो इस पर बैंक नियमित ब्याज देता रहेगा. यह ब्याज उसी खाते में जमा होता रहेगा. यह व्याज तभी मिलेगा, जब खाता सक्रिय होगा. लेकिन अगर कोई एफडी है और वह परिपक्व हो गया यानी जितने समय के लिए आपने एफडी कराई था वह समय पूरा हो गया तो उसके बाद उस पर कोई ब्याज नहीं मिलेगा। इसे बिना दावे वाली रकम के रूप में घोषित कर दिया जाएगा.

आरबीआई का 100 दिन का अभियान

हाल में आरबीआई ने बैंकों से कहा है कि वे उन बिना दावे वाली रकम के जमाकर्ताओं को खोजें जिनका कोई पता नहीं है. इसके लिए 100 दिन का अभियान एक जून से चालू किया गया है. इसमें शीर्ष 100 जिलों के 100 जमाकर्ताओं को खोजा जाएगा और उनको उनकी रकम दी जाएगी.

बहुतेरे लोग अपना पता बदल देते हैं, मोबाइल नंबर बदल देते हैं, पर वे इसकी सूचना बैंक को नहीं देते हैं. इसका नुकसान यह है कि बैंक पुराने रिकॉर्ड के आधार पर ही आपको चेकबुक, डेबिट कार्ड या कोई भी पत्र व्यवहार करता है तो इसका आपको पता नहीं चलता है. किसी भी स्थिति में ऐसे बदलावों की जानकारी बैंक को देना अनिवार्य और फायदेमंद है. हमने आपको उपर बता दिया हैं कि कैसे आपका निष्क्रिय खाता चालू हो सकता है और इसके लिए क्या किया जा सकता है.

बैंकों के पास इस समय बिना दावे वाली 35,000 करोड़ की रकम पड़ी है. ऐसा इसलिए होता है क्योंकि लोग किसी भी परिवर्तन की जानकारी बैंक को नहीं देते.

श्रीजय मंडपे
क्षेत्रीय प्रमुख
सेन्ट्रल बैंक ऑफ इंडिया

अदावाकृत खातों का सक्रियकरण

प्रस्तावना

आपने ऋण का एनपीए होना तो सुना ही होगा लेकिन जमा को एनपीए होते हुए देखा सुना है कभी? नहीं सुना होगा. नया मामला है. हाल ही में बैंकों ने भारतीय रिजर्व बैंक को लगभग 35 हजार करोड़ रुपए ट्रांसफर किए हैं. आपको आश्चर्य होगा कि यह राशि वह अदावाकृत राशि थी जिसे आप लावारिस राशि भी कह सकते हैं जो बैंकों के उन ग्राहकों की थी जो अपनी राशि जमा करके या तो भूल गए या मृत हो गए और वे कोई नामांकन नहीं कर पाए या उस राशि का कोई दावेदार नहीं रहा या उनका कहीं बाहर ट्रांसफर हो गया या किसी और कारण से 10 सालों तक बैंक के पास जमा रह गई थी. इसी राशि को जमा का एनपीए कहा जा रहा है. ऋण में एनपीए होने पर बैंकों को उतनी राशि का प्रावधान करना पड़ता है जो सीधे इनके लाभ से नामे होता है और जमा में एनपीए होने पर यह राशि आरबीआई को भेजनी पड़ती है जिससे बैंक का उतनी राशि से डिपॉजिट कम हो जाता है. आपको पता ही होगा कि बैंकों का पूरा कारोबार जमा राशियों से ही शुरू होता है. यह स्थिति भी बैंकों के लिए नुकसानप्रद है. यह स्थिति दुनिया भर के बैंकों में बनी हुई है. इसे कुछ इस तरह से भी समझ सकते हैं कि जब भी किसी जमा खाते में सालों तक ग्राहक द्वारा या उसके मेंडेट द्वारा कोई जमा या नामे नहीं किया जाता है तो खाता अपरिचालित स्थिति में चला जाता है और यह स्थिति अगर 10 वर्ष तक बनी रहती है और उसका कोई दावेदार बैंक से संपर्क नहीं करता है तो बैंक इस खाते को अदावाकृत यानि लावारिस मानते हुए इसकी राशि को आरबीआई को ट्रांसफर कर देता है.

इस लेख में हम क्रमश: आरबीआई, बैंक एवं ग्राहक के नजरिए से अदावाकृत खातों के सक्रियकरण पर चर्चा करेंगे.

आरबीआई –

भारतीय रिजर्व बैंक का मानना है कि सार्वजनिक एवं निजी क्षेत्र के बैंकों का यह योगदान महत्वपूर्ण है. यह इस बात का भी संकेत है कि बैंक उपभोक्ता हितों को लेकर बेहद सतर्क दृष्टि रखते हैं. भारतीय रिजर्व बैंक ने वर्ष 2014 में Depositor Education and Awareness Fund (DEAF) योजना की स्थापना की थी. असल में बैंकों के पास ऐसी रकम हमेशा से चिंता का कारण रही है, जिनका कोई दावेदार नहीं है. लोग पैसा जमा किये और भूल गए. परिवार में किसी को बताया नहीं और असमय दुनिया से चले गए. ऐसी रकम बैंक इस इंतजार में अपने पास रखते कि न जाने कब कौन दावेदार आ जाए.

इस फंड की स्थापना से सार्वजनिक और निजी, दोनों ही क्षेत्र के बैंकों की इस समस्या का समाधान हो गया. उन्हें अपने पास पैसा रखने की मजबूरी नहीं है. वे केंद्रीय बैंक की ओर से तय दिशानिर्देशों के मुताबिक लावारिस रकम इस फंड में जमा कर रहे हैं और जब भी जरूरत हो रही है, मतलब दावेदार के सामने आने पर उसे वापसी की प्रक्रिया शुरू कर दे रहे हैं.

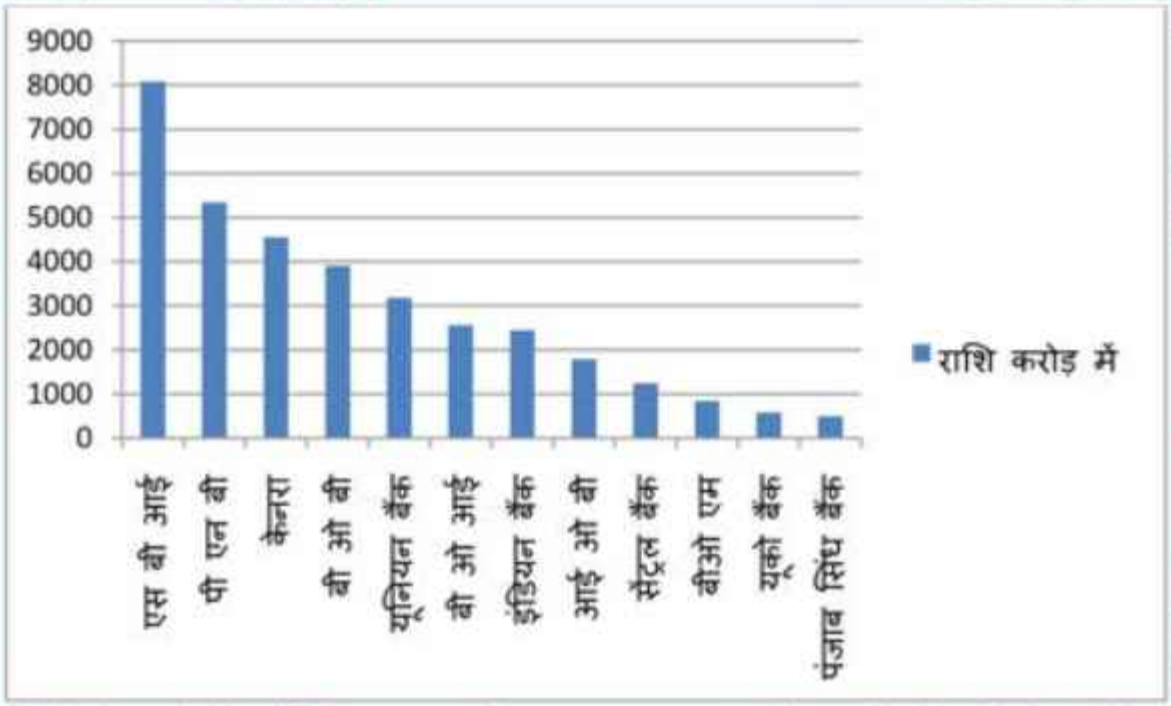
ऐसी रकम के उचित दावेदारों का पता लगाने के लिए भारतीय रिजर्व बैंक ने **'100 Days 100 Pays' ''सौ दिन सौ भुगतान''** नामक एक अभियान शुरू किया है जो 1 जून 2023 से शुरू होकर 8 सितंबर 2023 तक चलने वाला है. केंद्रीय बैंक ने सभी बैंकों से कहा है कि वे अपने क्षेत्राधीन प्रत्येक जिले में कम से कम सौ लावारिस जमा धन के दावेदारों का पता करें और जमा रकम उन्हें वापस करें. केंद्रीय बैंक ने इसके लिए अलग से एक पोर्टल भी लॉन्च किया है, जिससे जरूरतमंदों का पैसा उन्हें वापस मिल सके और इसमें पूरी पारदर्शिता भी बनी रहे. इसके तहत बैंकों को टारगेट भी दिए गए हैं. इसके तहत हमारे बैंक के नागपुर क्षेत्र से लगभग 3 करोड़ की राशि आरबीआई को गई है. जिसे हमें उनके सही मालिकों तक पहुंचाना है. एक सामाजिक दृष्टिकोण भी इसमें नजर आता है. इन खाता धारकों में से कई काफी जरूरत मंद भी हो सकते हैं. यह राशि मिलने से उनकी कुछ बेहतरी हो सकती है. जैसे जैसे ग्राहक हमारे पास आते जा रहे हैं हम उनकी राशि उन्हें वापिस कराते जा रहे हैं.

रिज़र्व बैंक ने बैंकिंग रेग्युलेशन एक्ट के सेक्शन 26 ए के तहत वर्ष 2014 में डिपॉजिटर एजुकेशन एंड अवेयरनेस फंड (DEAF) स्कीम शुरू करने की घोषणा की. तब से लगातार इसी योजना से बैंक सही दावेदारों को भुगतान कर रहे हैं. असल में बैंक इस तरह की राशि प्रति माह रिज़र्व बैंक में जमा कर देते हैं. पहले बैंकों द्वारा यह जानकारी वार्षिक आधार पर दिसंबर माह में दी जाती थी.

इस फंड की स्थापना से पहले सभी बैंक परेशानी में आ जाते थे. पर, अब रिज़र्व बैंक ने यह काम आसान बना दिया है. यह फंड लावारिस जमा धन उचित दावेदारों को वापस करने में महत्वपूर्ण भूमिका अदा कर रहा है. इस फंड की स्थापना का उद्देश्य यही था कि जमाकर्ताओं और बैंकों का हित सुरक्षित रहे और वे जागरूक रहें. इसका मुख्य उद्देश्य जमाकर्ताओं के हितों की सुरक्षा और जागरूकता फैलाना है. इस फंड की स्थापना के बाद से रिज़र्व बैंक ने वित्तीय साक्षरता पर भी जोर दिया. इसके लिए बैंकों ने विभिन्न माध्यमों से लगातार अनेकों जागरूकता अभियान किए हैं .

हाल ही में आरबीआई के गवर्नर ने एक केंद्रीयकृत वेब पोर्टल UDGAM (unclaimed deposits-gateway to access information) लाँच किया है ताकि आम आदमी विभिन्न बैंकों में जमा अपने अदावाकृत खातों का पता आसानी से लगा सकें.

देश के सार्वजनिक क्षेत्र के सभी बैंकों ने मिलकर 31 मार्च 2023 तक लगभग 35012 करोड़ रुपये इस फंड में जमा कराए. प्राइवेट बैंक भी इस मामले में पीछे नहीं रहे. उन्होंने भी 6087 करोड़ रुपये रिज़र्व बैंक को इस फंड के लिए उपलब्ध करवाए.



बैंक –

अगर कोई खाता एक वर्ष तक लेनदेन से दूर रहता है तो उस खाते को निष्क्रिय खाता कहा जाता है और यही स्थिति अगर 2 वर्ष तक रही तो इस खाते को अपरिचालित खाता कहा जाता है, अपरिचालित खाते की स्थिति में इस खाते को फ्रीज़ कर दिया जाता है. इस खाते में जमा तो हो सकता है लेकिन नामे नहीं हो सकता है. इसके लिए ग्राहक को उचित केवायसी के साथ खाते को परिचालित करने हेतु बैंक से अनुरोध करना होता है. यह स्थिति बैंक के लिए सहज नहीं होती, अक्सर देखा गया है कि इन अपरिचालित खातों में फ्रॉड भी होते रहते हैं. अक्सर बैंक स्टाफ या ग्राहक या कोई बाहरी व्यक्ति इसमें संलग्न पाया गया है. बैंक की छबि इससे प्रभावित होती है. इसके अलावा इन खातों की देखभाल के लिए अतिरिक्त स्टाफ लगाना पड़ता है जिनकी कमी से सभी बैंक जूझ रहे हैं. इस खातों को सक्रिय करने के लिए बैंक स्टाफ को भी जागरूक होने की आवश्यकता है. खाता अपरिचालित होते ही ग्राहक से सीधे, पत्र, मेल या एसएमएस के माध्यम से संपर्क करना शुरू कर देना चाहिए. बैंकों को अपनी शाखा में इसके बैनर पोस्टर भी लगाने चाहिए एवं जागरूकता कार्यक्रम आयोजित करने चाहिए. हमारी बैंक से लगभग 1240 करोड़ रुपए आरबीआई को ट्रांसफर हुए हैं. यह हमारा नुकसान है. हमारा जमा इतने रुपए से कम हो गया.

इस राशि का सही दावेदार जब बैंक आता है तो बैंक उसके केवायसी से संतुष्ट होने के पश्चात उसकी राशि का भुगतान नॉमिनल खाते से कर देता है और इस राशि को आरबीआई से क्लेम करके वापस ले लिया जाता है. इससे बैंक को इस राशि को संभालने की झंझट नहीं रहती. इस योजना के बाद से इस प्रकार के फ्रॉड भी काफी कम हो गए हैं.

जितने अधिक खाते सक्रिय होंगे, उतना अधिक बैंक को लाभ होगा, एक तो यह राशि आरबीआई से बैंक के पास आ जाएगी, दूसरे ग्राहक को भी आश्चर्य मिश्रित खुशी होगी जिससे वह बैंक से और अधिक जुड़ पाएगा. आरबीआई इस राशि पर 3% ब्याज भी अदा करती है. बैंक अपने एवं आरबीआई के पोर्टल की जानकारी सभी को दे सकता है. इससे बैंक का काम भी आसान हो जाएगा. इस वेब पोर्टल पर जाकर किसी भी बैंक से किसी भी व्यक्ति के नाम को सर्च कर पता कर सकते हैं कि उस व्यक्ति का किस बैंक मे अदावाकृत खाता है.

ग्राहक –

यह स्थिति ज्यादातर बुजुर्गों के साथ बनती है. वे कई बार कोई नामांकन भी नहीं कराते हैं. कई बार बच्चों को या रिश्तेदारों को भी पता नहीं होता है कि उनका कोई बैंक खाता भी है. अँग्रेजी में एक बहुत अच्छी लाइन है buyers be aware यानि खरीददारों/**ग्राहकों जागरूक रहो.** जागरूक ग्राहक हमेशा फायदे में रहता है. ग्राहक स्वयं भी जागरूक रहें और जागरूकता भी फैलाए। बैंक के ग्राहक को चाहिए कि वह अपने बैंक खाते से लेन देन करता रहे. आवश्यक नहीं होने पर भी वर्ष मे 2–4 बार बैंक के चक्कर लगा लें और कुछ जमा निकासी कर लें. बुजुर्गों को चाहिए कि वे अपनी वित्तीय स्थिति और बैंक, बीमा खाते या अपने निवेशों की जानकारी अपने बच्चों या विधिक उत्तराधिकारियों को अवश्य दें. साथ ही सभी ग्राहकों को अपने बैंक खातों में नामांकन अवश्य कराना चाहिए.

ग्राहक आरबीआई या बैंकों की साईट पर उपलब्ध वेबपोर्टल पर जाकर स्वयं का या किसी का भी अदावाकृत खाता पता कर सकता है. जैसे कि अगर हमारे बैंक का पता करना है तो CBI Unclaimed Deposits List टाईप करें. अगर वह राशि उनसे संबन्धित है तो वे क्लेम फॉर्म, केवायसी एवं बैंक दस्तावेज़ बैंक में लाकर अपनी राशि प्राप्त कर सकते हैं.

सुझाव –

1. ऋण वसूली एजेन्ट की तर्ज पर इस कार्य हेतु भी एजेंसियों की मदद ली जा सकती है
2. बैंकों में कार्यरत बीसी बीएफ से यह कार्य बेहतर रूप से किया जा सकता है
3. समाचार पत्र, टेलीविजन व अन्य संचार माध्यमों का प्रयोग कर जागरूकता फैलाई जा सकती है
4. बैंकों द्वारा एसएमएस, ईमेल, पोस्टर, बैनर, नुक्कड़ नाटक, वॉल पेंटिंग आदि का प्रयोग कर जागरूकता फैलाई जा सकती है
5. स्कूलों कॉलेजों में इस संबंध में कार्यक्रम आयोजित किए जा सकते हैं.
6. इसमें बेहतर कार्य करने वाले बैंकों को आरबीआई द्वारा प्रोत्साहन भी घोषित किया जा सकता है

उपसंहार

जब रू. 35012 करोड़ की राशि की जानकारी सरकार को लगी तो वह भी इस बड़ी मात्रा को देखकर चकित थी इसलिए सरकार द्वारा तुरंत निदेश जारी किए गए कि किसी भी स्थिति में जमाकर्ताओं के हित सुरक्षित रहें. कुल मिलाकर अदावाकृत खातों का सक्रियकरण बैंक व ग्राहक दोनों के हित में है. इससे खाते की राशि उचित व्यक्ति के पास पहुंचेगी. ग्राहक या उसके उत्तराधिकारी लाभ में होंगे एवं बैंक भी सहज ही लाभ की स्थिति में होंगे. इसकी अधिकाधिक जागरूकता फैलाने की आवश्यकता है ताकि बैंक व ग्राहक दोनों जागरूक हों. सरकार एवं आरबीआई की यह पहल प्रशंसा योग्य है. एक बैंकर के रूप में हम इस योजना का अधिकतम प्रचार प्रसार कर रहे हैं.

अनिल चौबे
वरिष्ठ प्रबन्धक राजभाषा
सेन्ट्रल बैंक ऑफ इंडिया,
क्षेत्रीय कार्यालय नागपुर

डिजिटलीकरण में कर्मचारियों की भूमिका

किसी भी प्रकार की सूचना को या किसी भी प्रकार के दस्तावेज को डिजिटल रूप में सुरक्षित रखने की प्रक्रिया को हम डिजिटलीकरण कहते है. आज के आधुनिक समय में इसका महत्व बहुत अधिक है क्योंकि किसी भी प्रकार की सूचना या डाटा को हार्ड फॉर्मेट में रखना बहुत ज्यादा समय तथा कागज आदि की बर्बादी होता है तो इसीसे बचने के लिए हम अपने सभी प्रकार के दस्तावेजों जैसे, अपने शिक्षा सम्बन्धी दस्तावेज, फ़ोटो, कम्पनी आदि के सभी दस्तावेजों आदि को अपने डिजिटल मशीनों या कम्प्यूटर में संग्रहित करके रखते हैं जिससे हमारा डाटा ज्यादा सुरक्षित रहता है और उसे प्राप्त करना बहुत ही आसान होता है.

डिजिटलाइजेशन / डिजिटलीकरण क्या है ?

डिजिटलीकरण समाज और अर्थव्यवस्था के डिजिटल परिवर्तन के लिए सामान्य शब्द है. यह एनालॉग प्रौद्योगिकियों की विशेषता वाले औद्योगिक युग से डिजिटल प्रौद्योगिकियों और डिजिटल व्यापार निष्कर्षों की विशेषता वाले ज्ञान और रचनात्मकता के युग में संक्रमण का वर्णन करता है.

डिजिटल प्रौद्योगिकियों का समाज पर व्यापक प्रभाव पड़ता है. डिजिटलीकरण हर उद्योग को वित्तीय नीति, रोजगार और प्रतिस्पर्धा जैसे क्षेत्रों पर प्रभावित कर रहा है. डिजिटलीकरण कोई नई घटना नहीं है. कई वर्षों से, इस अवधारणा में सामान्य रूप से तकनीकी विकास शामिल है, विशेषकर सूचना प्रौद्योगिकी में. डिजिटल अर्थव्यवस्था का असर कई क्षेत्रों पर पड़ रहा है. उदाहरण के लिए, कुछ सेवाएँ और उत्पाद जो पहले एनालॉग थे, जैसे यात्रा व्यवस्था, संगीत, फिल्म, अनुवाद और मीडिया डिजिटल हो रहे हैं.

डिजिटल तकनीक का स्वास्थ्य देखभाल, कानून प्रवर्तन, कला, शिक्षा, गतिशीलता और धर्म सहित हमारी संस्कृति के बुनियादी पहलुओं पर भी सकारात्मक प्रभाव पड़ता है. उदाहरण के लिए, स्वास्थ्य देखभाल उद्योग में तकनीकी प्रगति ने डॉक्टरों को वीडियो कॉन्फ्रेंसिंग जैसे माध्यमों का उपयोग करके आभासी वातावरण में मरीजों का इलाज करने का अवसर प्रदान किया है. कानूनी माहौल में वीडियो कॉन्फ्रेंसिंग भी एक महत्वपूर्ण भूमिका निभाती है. यह न्यायाधीशों को उन अपराधियों के मामलों को सुनने में सक्षम बनाता है जो सुरक्षा कारणों से अदालत कक्ष में प्रवेश नहीं कर सकते हैं.

डिजिटलीकरण और डिजिटल परिवर्तन ये सभी शब्द 2000 के दशक के उत्तरार्ध से बहुत प्रमुख रहे हैं. इनका परस्पर उपयोग किया जाता रहा है, अक्सर गलत कारणों से संभवतः उन्हें वह महत्व नहीं दिया गया जिसके वे हकदार हैं.

इनमें से कोई भी शब्द एक दूसरे के बिना अस्तित्व में नहीं है. अपनी स्थापना के बाद से ये तीनों कुछ हद तक एक जैसे हैं, पिछले कुछ वर्षों में इन्हें परिभाषित करने के तरीके में प्रगति और समायोजन हुए हैं.

डिजिटलीकरण एक वैचारिक शब्द है जो विभिन्न प्रकार के साहित्य से कई संबंध रखता है. यह एनालॉग चीजों का डिजिटल संस्करण बनाने का शब्द है. यह भौतिक पदार्थ को डिजिटल प्रारूप में परिवर्तित कर रहा है. उदाहरण के लिए कागजी दस्तावेज़, माइक्रोफ़िल्म छवियाँ, फ़ोटोग्राफ़ और बहुत कुछ बिट्स और बाइट्स में जो उन्हें परिभाषित करते हैं.

कुल मिलाकर, यह गैर–डिजिटल डेटा को डिजिटल प्रारूप में फिर से प्रस्तुत करने की सरल प्रक्रिया है जिसे कंप्यूटिंग सिस्टम द्वारा विभिन्न तरीकों से और विभिन्न कार्यों के लिए उपयोग किया जा सकता है. इस प्रकार, इस पूरी प्रक्रिया में, मूल दस्तावेज़ का कुछ भी खो नहीं जाता है. हालांकि कई मामलों में जगह खाली करने के लिए मूल वस्तु को नष्ट कर दिया जाता है, लेकिन किसी भी मामले में, यह डिजिटल रूपों में रहता है.

उदाहरण:

- बिलों, दस्तावेज़ों और फ़ाइलों को स्कैन करना
- मीटिंग मिनट्स और नोट्स को कागज से एक्सेल शीट में स्थानांतरित करना

डिजिटलीकरण की परिभाषा :

सरल शब्दों में डिजिटलाइजेशन को सामान्य रूप से इस प्रकार परिभाषित किया जा सकता है कि सभी प्रकार के डाटा को जैसे– दस्तावेज, इमेज, परिचय पत्र आदि को एक डिजिटल फार्मेट में बदलना.

कर्मचारियों के लिए यह महत्वपूर्ण क्यों है ?

डिजिटलीकरण के सभी उद्योगों पर प्रभाव पड़ने के साथ, डिजिटल साक्षरता आज के सबसे मूल्यवान व्यवसायिक कौशलों में से एक है. कर्मचारियों को यह समझने की आवश्यकता है कि प्रक्रियाओं और प्रणालियों को बेहतर बनाने के लिए प्रौद्योगिकी का उपयोग कैसे किया जा सकता है और ग्राहक संचार में इसका प्रभावी ढंग से उपयोग कैसे किया जा सकता है.

चाहे आपका व्यवसाय ग्राहकों के साथ व्यक्तिगत रूप से या ईमेल पर सौदा करता हो – आपके पास अभी भी एक ऑनलाइन उपस्थिति होगी जिसमें एक वेबसाइट और सोशल मीडिया प्रोफाइल शामिल हैं, दोनों को नियमित रखरखाव की आवश्यकता होती है.

प्रौद्योगिकी पर इस बढ़ती निर्भरता का मतलब अधिक साइबर हमले भी हैं – प्रत्येक संगठन को अपनी सुरक्षा नीतियां निर्धारित करते समय इस पर विचार करना चाहिए. हालाँकि डिजिटलीकरण सभी व्यवसायों पर लागू नहीं होता है (उदाहरण के लिए, वे जो आमने-सामने बातचीत पर ध्यान केंद्रित करते हैं), इसने वाणिज्य के लगभग हर पहलू को प्रभावित किया है.

डिजिटलाइजेशन की आवश्यकता क्यों है –

1. समय की बचत

जैसा की हम सभी जानते हैं कि किसी भी इंसान या किसी संगठन के द्वारा अपने सभी रिकार्ड तथा दस्तावेजों के कागज या हार्ड रूप रख रखाव में बहुत ज्यादा समय की बर्बादी होती है तथा इसमें बहुत अधिक पैसे की बर्बादी होती है. जबकि यदि हमारा डाटा डिजिटल फॉर्मेट में है तो उसे प्राप्त करना बहुत ही सरल होता है तथा इसमें समय की भी बचत होती है.

2. डाटा को चेंज करने में आसानी

डिजिटल रूप में रखे गये डाटा में हम जब भी चाहे बदलाव कर सकते हैं जबकि हार्ड रूप में ऐसा करना हमेशा संभव नहीं

होता. डिजिटल रूप में रखे गए डाटा को कभी भी बहुत जल्दी चेक किया जा सकता है जबकि कागजी रूप में स्टोर डाटा को चेक करने में बहुत समय लगता है.

3. विश्लेषण में सहायक

अधिकतर किसी संगठन में बार बार अपने ग्राहकों, कर्मचारियों, लेनदारों तथा देनदारों आदि के लेखों को जांचने के लिए भी डिजिटल फॉर्मेट में सेव किया गया डाटा ही सबसे अधिक अच्छा रहता है. जिसमें डाटा का ऑडिट करना बहुत ही आसान होता है.

4. डाटा की सुरक्षा

डिजिटल रूप में रखे गए डाटा का खराब होने या बेकार होने का खतरा बहुत ही कम होता है तथा इसको कुछ ही पलो में एक से अधिक रूप में सुरक्षित करके रखा जा सकता है. इसमें हमारे दस्तावेजों के आग या पानी आदि से नष्ट होने के खतरे को बिल्कुल कम किया जा सकता है. क्योंकि यह एक से ज्यादा तरीकों से अलग अलग उपकरणों जैसे हार्ड डिस्क, मेमोरी कार्ड, सीडी ड्राइव, और आजकल जो बिल्कुल नया है – गूगल ड्राइव जिसमें ऑनलाइन रूप में ही अपने डाटा को सुरक्षित रख सकते हैं.

5. डाटा के सभी रूप रखे जा सकते हैं

डिजिटल रूप में हम किसी भी तरह के डाटा को रख सकते हैं चाहे वह लिखित रूप में हो या दृश्य या श्रव्य रूप में हो. यदि हम अपने डाटा को ऑनलाइन ड्राइव में रखते हैं तो उसे हम इंटरनेट के जरिये कभी भी और कहीं भी प्राप्त कर सकते है.

6. अधिक विश्वसनीयता

डिजिटल रूप में रखा गया डाटा अधिक विश्वसनीय होता है क्योंकि उसमें गलती होने की संभावना कम होती है. जो डाटा मशीनों द्वारा तैयार तथा सेव किया जाता है वह अधिक प्रभावी व सही डाटा होता है.

7. कागज के इस्तेमाल में कमी

डाटा को डिजिटल रूप में रखने से कागज का इस्तेमाल कम किया जा सकता है. हर साल बहुत से पेड़ केवल कागज की पूर्ति के लिए काट दिए जाते हैं, जबकि हम अच्छी तरह से जानते हैं कि हमारे जीवन में **पेड़ों का महत्त्व** कितना अधिक होता है.
इन सभी कारणों के चलते यह स्पष्ट है कि आज के समय में अपने किसी भी तरह के डाटा या सूचना को डिजिटल फॉर्मेट में रखना कितना जरुरी है. डिजिटलीकरण हमारे कीमती समय को तो बचाता ही है साथ में यह कागजी कार्यवाही को भी कम करता है. इसलिए आज के समय में डिजिटलीकरण एक अहम् जरुरत बन चुका है.

डिजिटल रूप में हम किसी भी तरह के डाटा को रख सकते हैं चाहे वह लिखित रूप में हो या दृश्य या श्रव्य रूप में हो। यदि हम अपने डाटा को ऑनलाइन ड्राइव में रखतें हैं तो उसे हम इंटरनेट के जरिये कभी भी और कहीं भी प्राप्त कर सकते हैं. डिजिटल रूप में रखा गया डाटा अधिक विश्वसनीय होता है क्योंकि उसमे गलती होने की संभावना कम होती है.

समाज पर डिजिटलीकरण का प्रभाव

चार्ल्स डार्विन ने कहा था कि सबसे मजबूत वह नहीं है जो जीवित रहता है, न ही सबसे बुद्धिमान जो जीवित रहता है, यह वह है जो परिवर्तन के लिए सबसे अधिक अनुकूलनीय है. **डिजिटलाइजेशन आज के समय की मांग है.**

- हाल के वर्षों में – वर्ष 2000 के आसपास से – विभिन्न डिजिटल तकनीकों (मोबाइल इंटरनेट, कृत्रिम बुद्धिमत्ता, इंटरनेट ऑफ थिंग्स, आदि) को काफी हद तक विकसित किया गया है और विशेषज्ञ अनुप्रयोग से लोगों के रोजमर्रा के जीवन में परिवर्तन किया है.
- जिस प्रकार भाप इंजन के आविष्कार और बिजली के प्रसार ने समाज को बदल दिया है, उसी प्रकार डिजिटलीकरण ने अर्थव्यवस्था और समाज को बदल दिया है.
- डिजिटलीकरण प्रौद्योगिकी–प्रेरित है. डिजिटल नवाचार नई डिजिटल प्रौद्योगिकियों के आधार पर बनाए जाते हैं: नवोन्वेषी उपयोग के मामले एक ओर स्थापित कंपनियों द्वारा और दूसरी ओर स्टार्ट–अप और उद्यम पूंजी द्वारा संचालित होते हैं.
- इससे कागजी दस्तावेजों का उपयोग करने और अपने वेब पोर्टल पर फाइलों के साथ काम करने के लिए विभिन्न सार्वजनिक प्रशासन का डिजिटलीकरण हो रहा है, बाजार भी बहुत तेजी से बदल रहे हैं. संगीत और मीडिया उद्योग डिजिटलीकरण के प्रभावों का अनुभव करने वाले पहले व्यक्ति थे. खुदरा उद्योग ने इसका अनुसरण किया.
- आर्टीफिशियल इंटेलीजेंस और ब्लॉक चेन जैसी नई प्रौद्योगिकियां 2040 तक बिजनेस मॉडल और कंपनियों को पूरी तरह से बदलना जारी रखेंगी.

कंपनी में डिजिटलीकरण शीर्ष प्रबंधन के लिए एक विषय है. एबालिटिक्स इनोवेशन मैनेजमेंट सॉफ्टवेयर कंपनियों को डिजिटल परिवर्तन लाने में मदद करता है. एक कंपनी के भीतर, विभिन्न नवाचार नेटवर्क स्थापित और प्रबंधित किए जा सकते हैं, जो कंपनी के भीतर व्यवस्थित रूप से डिजिटलीकरण को आगे बढ़ाते हैं.

डिजिटल मार्केटिंग सेवाएँ लोगों को अधिक कुशल बनने में भी मदद करती हैं और इससे उत्पादकता बढ़ती है.
प्रौद्योगिकी हमें समय और पैसा बचाने में भी सक्षम बनाती है. इसने दुनिया को एकजुट करने और इसे एक डिजिटल गांव में बदलने में भी अच्छा काम किया है. यह बदले में लोगों को उनकी नस्लीय, सांस्कृतिक और महाद्वीपीय बाधाओं को दूर करने में सहायता करता है.

भारत ने अपने नागरिकों के लिए विभिन्न डिजिटल प्लेटफ़ॉर्म पेश किए हैं – MYGOV, MNREGA- SOFT, PAYGOVINDIA, प्रधानमंत्री जनधन योजना, स्मार्ट सिटीज़, ESANPARK, पासपोर्ट सेव प्रोजेक्ट, शाला दर्पण, आधार, डिजिलॉकर, आरोग्य सेतु आदि .

बैंकिंग जगत पर डिजिटलीकरण का प्रभाव

डिजिटलीकरण से बैंकिंग क्षेत्र भी अछूता नहीं रहा है. डिजिटलीकरण का बैंकिंग व्यवसाय पर इतना व्यापक प्रभाव पड़ा है कि किसी अन्य तरीके /मैनुअल आदि से वर्तमान में बैंकिंग व्यवसाय करने की कल्पना करना कठिन है. यह कोई रहस्य नहीं है कि इंटरनेट ने बैंकिंग व्यवसाय और समाज के लगभग हर पहलू को बदल दिया है, जिससे बैंकिंग तात्कालिक हो गई है, बैंकिंग जानकारी सुलभ हो गई है और मानव ज्ञान लगभग असीमित हो गया है. डिजिटलीकरण को हल्के में लेना आसान है, लेकिन विचार करें कि कंप्यूटर से पहले बैंकिंग कैसी थी, जीवन कैसा था, और आप देखेंगे कि हम इतने कम समय में कितनी दूर आ गए हैं.

इसके प्रभाव क्या हैं?

प्रौद्योगिकी लगातार विकसित हो रही है, यही कारण है कि बैंकिंग को भी डिजिटल रुझानों के साथ अद्यतन रहना चाहिए और अनुकूलन करने में सक्षम होना चाहिए. डिजिटलीकरण के कई प्रभाव हैं. एक के लिए, इसने अधिक वैश्विक अर्थव्यवस्था की अनुमति दी है, क्योंकि कोई भी व्यक्ति कम लागत पर दुनिया भर के किसी भी अन्य व्यक्ति के साथ बैंकिंग/व्यवसाय कर सकता है. परिणामस्वरूप, स्थानीय व्यवसाय ग्राहकों को अपने ब्रांड और उत्पादों के साथ बातचीत करने के लिए ऑनलाइन प्लेटफ़ॉर्म या भौतिक स्थान प्रदान करने में असमर्थता के कारण निगमों के साथ प्रतिस्पर्धा करने के लिए संघर्ष कर रहे हैं. हालाँकि, ऑनलाइन व्यवसायों को ऑर्डर पूरा करने और सामान का उत्पादन करने के लिए अभी भी भौतिक स्थानों की आवश्यकता होती है. इन मुद्दों को दूर करने के लिए, कुछ बड़ी कंपनियों ने छोटी कंपनियों के साथ साझेदारी की है ताकि वे अपने स्वयं के किसी अन्य स्थान के बिना उन्हें आपूर्ति कर सकें.

डिजिटलीकरण से कर्मचारियों का विकास

डिजिटलीकरण से व्यवसाय का विकास तो हुआ है, लेकिन कर्मचारियों की तकनीकी कुशलता, आय में वृद्धि हुई है. व्यवसाय और कर्मचारी एक दूसरे की प्रगति के साझेदार है. व्यवसाय में लागत में कमी होने से कर्मचारियों को वेतन, भत्तों, में बढोतरी से उनकी आय में वृद्धि हुई है. वर्क फ्रॉम होम की अवधारणा से कंपनियों की व्यवसाय लागत में कमी और कर्मचारियों के खर्चो में कमी हुई है. डिजिटल प्रगति ने खरीदारी से लेकर बिलों की देखभाल और दस्तावेज़ों के भंडारण तक सब कुछ आसान बना दिया है. और डिजिटलीकृत मीडिया ने लोगों के जीवन को बदलना बंद नहीं किया है; इसने बड़े और छोटे व्यवसायों को भी पूरी तरह से बदल दिया है. कई कंपनियाँ अब अपनी ऑनलाइन उपस्थिति के बिना सफल नहीं हो सकतीं, और यह सही भी है!

पीडब्लूसी के ग्लोबल कंज्यूमर इनसाइट्स सर्वे 2020 के अनुसार, इटली में कपड़ों और जूतों की खरीदारी में 65%, सेवाओं और खेल उपकरणों की खरीदारी में 57% और इलेक्ट्रॉनिक कार्यालय उपकरणों की खरीदारी में 44% की गिरावट आई है. कुल मिलाकर, अकेले घरेलू भोजन और वितरण क्षेत्र में औसतन 41% और स्वास्थ्य और सौंदर्य देखभाल उत्पाद क्षेत्र में 35% की गिरावट देखी गई.

उपरोक्त की पुष्टि करते हुए, वही शोध यह भी दर्शाता है कि भोजन के अलावा अन्य सभी उत्पादों की ऑनलाइन खरीदारी में मोबाइल के माध्यम से 45%, पीसी के माध्यम से 41% और टैबलेट के माध्यम से 33% की वृद्धि हुई, जबकि इन-स्टोर खरीदारी में 50% की कमी आई. दूसरी ओर, जहां तक खाद्य उत्पादों का सवाल है, अगर कोविड-19 से पहले केवल ऑनलाइन खरीदारी 9% थी, तो अब 63% उत्तरदाताओं का कहना है कि वे ऑनलाइन के माध्यम से अधिक खरीदारी करते हैं और 89% का कहना है कि वे महामारी के बाद भी ऐसा करना जारी रखेंगे. महामारी का अंत डिजिटल में परिवर्तन के उद्देश्य से एक नया बाज़ार रुझान बनाता है. इसमें कोई आश्चर्य की बात नहीं है कि ग्रैनारोलो जैसे कई बड़े ब्रांडों ने अपनी ऑनलाइन ई-कॉमर्स साइट खोलने का फैसला किया है.

कर्मचारियों के लिए डिजिटलीकरण कितना प्रभावी रहा है?

विकास लगातार धीरे-धीरे आगे बढ़ता रहता है जिसमें सार्वजनिक-निजी भागीदारी (पीपीपी) प्रमुख भूमिका निभाती है. प्रौद्योगिकी, सहयोग, कनेक्टिविटी टूल के क्षेत्र में प्राप्त विकास के साथ-साथ प्रबंधन अभ्यास में परिवर्तन रोजमर्रा की जिंदगी को संवेदनशील रूप से प्रभावित करते हैं, जो प्रत्येक व्यक्ति के जीवन में डिजिटलीकरण के महत्व को दर्शाता है. हालाँकि, ग्रामीण क्षेत्रों में बिजली की प्रतिबंधित और सीमित पहुंच डिजिटल प्रौद्योगिकी के आगे विकास में एक बड़ी बाधा बनी हुई है. स्मार्ट सिटी बनाने का मिशन रियल एस्टेट उद्योग, निर्माण, इस्पात और कंक्रीट उद्योग के साथ-साथ बुनियादी ढांचा क्षेत्र को भी बढ़ावा देगा. 'मेक इन इंडिया' और 'डिजिटल इंडिया' तकनीकी क्षेत्र के लिए नए अवसर लेकर आए. विदेशी कंपनियाँ भारत में निवेश कर रही हैं और उत्पादों के निर्माण के लिए अपने संयंत्र स्थापित कर रही हैं जो इस देश में बेचे जा रहे हैं और निर्यात भी किए जा रहे हैं. डिजिटलीकरण प्रक्रिया ने कोई भी क्षेत्र अछूता नहीं छोड़ा है, लेकिन कानूनी स्पष्टता की कमी कुछ क्षेत्रों पर नकारात्मक प्रभाव डालती है. राजनीतिक ढांचे के कारण अमेजन और उबर जैसी कंपनियों को सांप्रदायिक अधिकारियों के साथ कई विवादों का सामना करना पड़ा, जो डिजिटल युग में व्यवसाय के लिए उपयुक्त नहीं है.

कर्मचारियों को डिजिटलीकरण के फायदे और नुकसान

डिजिटलीकरण से कई फायदे हुए हैं, उनमें से कुछ हैं:

1. पहुंच असीमित और कालातीत है और इसे कहीं से भी किया जा सकता है, बशर्ते उपयोगकर्ता ने पहुंच की अनुमति दी हो और पर्याप्त इंटरनेट कनेक्शन हो.
2. डिजिटलीकरण बड़ी मात्रा में संसाधनों का संरक्षण करता है और इस प्रकार, यह कहीं अधिक पर्यावरण-अनुकूल है.
3. व्यवसाय की बातचीत और लेन-देन पूरी तरह से बदल गया है जिससे यह बहुत आसान और लाभदायक हो गया है.
4. नीतियों और योजनाओं की पहुंच पहले से कहीं अधिक है.
5. इसकी दक्षता में सुधार हुआ है क्योंकि एक डिजिटल स्मार्ट फैक्ट्री सभी मोर्चों पर अधिक कुशल है.
6. इसने समय को पूरी तरह से कम कर दिया है क्योंकि ग्राहक तेजी से अनुरोध करते हैं और डिजिटल सिस्टम और रणनीतियों के साथ थ्रूपुट को कुशलतापूर्वक प्रबंधित करते हैं.
7. इससे आर्थिक विकास को काफी बढ़ावा मिला है.

डिजिटलीकरण में कर्मचारियों की भूमिका

प्रौद्योगिकियों तक आसान पहुंच डिजिटल प्रौद्योगिकियों को व्यवसायों के सभी स्तरों पर उपलब्ध करा रही है, चाहे वह छोटा हो या बड़ा. डिजिटल सक्षमता (समय की आवश्यकता के अनुसार) किसी संगठन को समय के साथ बने रहने में मदद करेगी. प्रौद्योगिकियों के विकास में तेजी से वृद्धि के साथ, जो संगठन इसे अपनाने में असमर्थ हैं, उनके पिछड़ने की संभावना है. व्यवसायिक मामला बनाने के कुछ और कारण यहां दिए गए हैं;

1. फॉरेस्टर रिसर्च के एक सर्वेक्षण के अनुसार, यह अनुमान लगाया गया है कि वर्ष 2020 तक राजस्व का आधा हिस्सा डिजिटल परिवर्तन से प्रेरित होगा.
2. जिन कंपनियों ने इस बदलाव को अपनाया है, उन्होंने दूसरों की तुलना में 26% अधिक लाभदायक वृद्धि देखी है
3. पुरानी विरासत प्रणाली के कारण बढ़ी हुई दक्षता की अपनी सीमाएँ हैं और यह संभावित विकास को धीमा करके व्यवसाय को रोक रही है.
4. मोबाइल उपकरणों और प्रौद्योगिकियों के आगमन के साथ, व्यक्ति सूचना सुनामी के युग में जी रहा है जो तेजी से निर्णय लेने में सक्षम बना रहा है.

डिजिटलीकरण का समाज पर नकारात्मक प्रभाव

डिजिटल तकनीक का समाज पर भी कुछ नकारात्मक प्रभाव पड़ रहा है. उदाहरण के लिए, डिजिटल प्रौद्योगिकी में प्रगति अक्सर रचनात्मकता के विनाश का कारण बनती है. नई तकनीकों के आने से अर्थव्यवस्था पर भी नकारात्मक प्रभाव पड़ सकता है. उदाहरण के लिए, टेलीविजन लोगों के एक दिन के कई उत्पादक घंटे बर्बाद कर सकता है. डिजिटल प्रौद्योगिकी के दीर्घकालिक परिणाम हमेशा पूर्वानुमानित नहीं होते हैं.

निष्कर्ष के तौर पर डिजिटलीकरण का अर्थ लोगों और व्यवसाय के लिए सेवाओं को बेहतर बनाने के लिए ऑनलाइन तकनीकों का उपयोग करना है. इसका मतलब सरकार के काम करने के तरीके को नया स्वरूप देने के लिए डेटा और प्रौद्योगिकी का उपयोग करना भी है. हम मूल्य कैसे प्रदान करते हैं, हम कैसे काम करते हैं और हमारी संगठनात्मक संस्कृति पर पुनर्विचार करने के लिए डेटा और प्रौद्योगिकी का उपयोग करेंगे.

यदि आप 21वीं सदी के डिजिटल कौशल नहीं सीखते हैं, तो भविष्य की चुनौतियों से तालमेल बिठाना आपके लिए कठिन होगा. आज ही अपने आप को नया रूप देना शुरू करें, अन्यथा आप भविष्य की तकनीक में अप्रासंगिक हो जाने का जोखिम उठाएँगे.

उपसंहार

डिजिटलीकरण के क्या लाभ हैं? कुछ ही महीनों में, COVID–19 के प्रसार से जुड़ा वैश्विक स्वास्थ्य संकट व्यवसायों, सरकारों और नागरिकों द्वारा कुछ सेवाओं को उपलब्ध कराने और उनका उपयोग करने के तरीके में संरचनात्मक परिवर्तन करने में कामयाब रहा है, जिससे हर कोई डिजिटल परिवर्तन को आगे बढ़ा रहा है. मैकिन्से के एक अध्ययन से पता चला है कि उपभोक्ताओं के साथ कंप्यूटर–आधारित बातचीत का मौजूदा स्तर 2023 तक अपेक्षित रुझान से 3 साल आगे है, और कैसे कंपनियों ने अपने उत्पादों को आंशिक या पूरी तरह से डिजिटल बनाए रखने के लिए निर्धारित समय से 7 साल पहले विकसित किया है. बाज़ार में प्रतिस्पर्धी. इसके अलावा, डिजिटलीकरण ने दैनिक जीवन के सभी संगठनात्मक पहलुओं को भी प्रभावित किया है, जिससे श्रमिकों और छात्रों को अपने कार्यों को दूर से पूरा करना पड़ रहा है और स्वाभाविक परिणाम के रूप में, गतिशीलता में कमी आई है और साथ ही ऑनलाइन खरीदारी में वृद्धि हुई है. ऑनलाइन बैंकिंग को एक नया आयाम मिला है.

निष्कर्षतः हम कह सकते हैं कि डिजिटलीकरण से हमें बहुत लाभ हुआ है. पिछले वर्षो विशेषकर कोविड–19 के दौरान मजबूरी में ही **डिजिटलीकरण** ने हमें बहुत सिखाया है और हमारे देश में इस क्षेत्र में सभी वर्गों की इससे बहुत प्रगति हुई है.

सुनील कुमार शर्मा
मुख्य प्रबंधक (राजभाषा)
आंचलिक कार्यालय, लखनऊ

राईट ऑफ खातों में वसूली

ऋण को राइट–ऑफ करना एक ऐसा माध्यम है जिसका इस्तेमाल बैंक अपनी बैलेंस शीट को साफ सुथरा करने के लिए करते हैं. इसे खराब ऋण या नॉन परफार्मिंग एसेट्स (NPA) के मामलों में लागू किया जाता है. यदि कम से कम लगातार तीन तिमाहियों के लिए पुनर्भुगतान के कारण कोई ऋण खराब हो जाता है, तो जोखिम (ऋण) को राइट ऑफ में डाल दिया जा सकता है.

एक लोन राइट–ऑफ किसी भी ऋण के प्रावधान के लिए बैंकों द्वारा जमा किए गए धन को मुक्त करता है. ऋण के लिए प्रावधान बैंकों द्वारा अलग रखी गई ऋण राशि के एक निश्चित प्रतिशत को संदर्भित करता है. भारतीय बैंकों में ऋण के प्रावधान का स्टैंडर्ड रेट बिज़नेस सेक्टर और कर्जदार की चुकौती क्षमता के आधार पर 5–20 प्रतिशत से भिन्न होती है. NPA के मामलों में, बेसल–III मानदंडों के अनुसार 100 प्रतिशत प्रावधान करना आवश्यक है. सरकारी बैंकों को कम से कम 40 फीसदी तक की वसूली करनी चाहिए। इस समय बट्टे खाते से वसूली दर 15 फीसदी से कम है. बट्टे खाते का मतलब राइट ऑफ से है, जिसे कभी भी बैंक वसूल सकते हैं. मार्च, 2023 को समाप्त पांच वर्षों के दौरान इन बट्टे खातों में से केवल 14 फीसदी की ही वसूली हो पाई

राइट ऑफ लोन क्या हैं?

किसी ऋण या संपत्ति को राइट ऑफ़ में डालने का अर्थ है कि यह विचार करना कि इसका भविष्य का कोई मूल्य नहीं है या अब उद्देश्य पूरा नहीं करता है. एक नॉन परफार्मिंग एसेट्स को तब राइट ऑफ में डाल दिया जाता है जब वसूली के सभी रास्ते समाप्त हो जाते हैं और देय ऋण की वसूली की संभावना बहुत कम होती है.

बैलेंस शीट को क्लीन–अप करने के लिए, इस तरह के सभी ऋण एक बार सभी के लिए राइट ऑफ में डाल दिए जाते हैं. यह एक नियमित प्रैक्टिस है जो बैंक अपनी बैलेंस शीट को क्लीन–अप करने के साथ–साथ कर दक्षता हासिल करने के लिए करते हैं.

हालांकि बुरे ऋणों को राइट ऑफ में डाल दिया जाता है, ऐसे ऋणों के कर्जदार चुकौती के लिए उत्तरदायी रहते हैं. ऐसे कई मामले हैं जब ऐसे खराब अकाउंट को राइट ऑफ में डाल दिया गया था लेकिन ऋण की वसूली की गई थी. हालांकि, ऐसे अकाउंट की वसूली कानूनी तंत्र के तहत निरंतर आधार पर होती है.

डेब्ट्स राइट–ऑफ एक बैंक की बैलेंस शीट में खराब संपत्ति के अंत का संकेत देता है. इसे समकक्ष निधि द्वारा प्रतिस्थापित किया जाता है. बैंक का वित्तीय विवरण इंगित करेगा कि राइट ऑफ में डाले गए ऋणों की भरपाई किसी अन्य तरीके से की जाती है. बैंक की बैलेंस शीट को क्लीन करने के लिए इसकी जरूरत होती है. बैलेंस शीट की सफाई का मतलब है कि खराब संपत्ति को बदल दिया गया है.

बैंकिंग दृष्टिकोण से, राइट–ऑफ़ शब्द केवल एक अकाउंटिंग शब्द है. इसका मतलब यह है कि बैंक या ऋणदाता उस पैसे की गणना नहीं करता है जो कर्जदार पर बकाया है. एक डिफॉल्टर के लिए राइट ऑफ में डालने का अर्थ यह नहीं है कि उसे क्षमा कर दिया गया है; बल्कि उसके खिलाफ कानूनी कार्रवाई जारी रहेगी.

आप राइट–ऑफ़ का विश्लेषण तीन दृष्टिकोण से कर सकते हैं:

- बैंक– इसकी बैलेंस शीट में सुधार होगा.
- डिफॉल्टर – कानूनी कार्रवाई सहित परिणामों का सामना करना पड़ता है.
- आम जनता – यह धारणा बनाएं कि कर्ज लेना और न चुकाना लाभदायक है.

बैंक के दृष्टिकोण से शब्द को समझने का सबसे अच्छा तरीका है, क्योंकि यह बैंक है जिसे बोझ उठाना चाहिए, प्रक्रिया शुरू करनी चाहिए और उन पर खराब संपत्तियों को बदलने की जिम्मेदारी होती है. खराब संपत्ति की समस्या बैंक के लिए अस्तित्व का मुद्दा है. राइट–ऑफ के माध्यम से खराब संपत्ति को बदलना एक रास्ता है.

राइट ऑफ में डाले गए ऋणों की भरपाई कैसे?

- प्रतिभूतिकरण – यहां बैंक डिफॉल्टर की अंतर्निहित संपत्ति (भवन, मशीनरी आदि) को एक परिसंपत्ति पुनर्निर्माण कंपनी को बेच सकता है. इस प्रक्रिया में भी ऋण के केवल एक भाग (कभी–कभी– प्रमुख भाग) की ही वसूली की जा

सकती है. शेष की भरपाई बैंक द्वारा अपने लाभ से या पूंजी से की जानी चाहिए.

- प्रोविजनिंग – यहां, बैंक राइट ऑफ में डाली गई संपत्ति की भरपाई के लिए मुनाफे और अन्य धन का उपयोग करता है.
- पूंजी – यहां, बैंक अपने शेयरधारकों के योगदान (नई पूंजी के रूप में) का उपयोग राइट ऑफ में डाली गई संपत्ति की भरपाई के लिए करता है. हालिया पुनर्पूंजीकरण इस प्रारूप के लिए एक उदाहरण है.

अर्थव्यवस्था पर कर्ज के राइट ऑफ का प्रभाव

ऋण राइट–ऑफ बैंकों को राहत देता है क्योंकि यह व्यवसाय करने के लिए अपने ब्लॉक धन को पुनः प्राप्त करता है. यदि राइट–ऑफ वांछनीय तरीके से किया जाता है तो बैंक सबसे महत्वपूर्ण लाभार्थी है. बहुत अधिक समय के लिए बहुत अधिक धन ब्लॉक होने से बैंक की ऋण देने की क्षमता कम हो जाएगी.

अर्थव्यवस्था के लिए, एक बार जब बैंक मजबूत हो जाते हैं, तो वे अधिक आर्थिक गतिविधियों को वित्तपोषित कर सकते हैं और इस तरह, राइट–ऑफ़ से अर्थव्यवस्था को लाभ होगा.

डिफॉल्टर के लिए कानूनी कार्रवाई उस पर दबाव बनाएगी और उसकी वित्तीय गतिविधियों पर रोक लगा दी जाएगी.

निष्कर्ष

जब कोई बैंक ऋण की वसूली करने में सक्षम नहीं होता है तो ऋण खराब हो जाता है और उसे राइट ऑफ में डाल दिया जाता है.

- अपनी बैलेंस शीट को साफ करने और अपनी कर देयता को कम करने के लिए, बैंक अक्सर खराब ऋणों को राइट ऑफ में डाल देते हैं, जो बैंक के लिए सबसे समान रूप से खराब ऋण है. अनिवार्य रूप से बैंकों को आमतौर पर खराब ऋणों के लिए भंडार रखने की आवश्यकता होती है. कर्ज का कुछ हिस्सा वसूल कर लिया जाता है और कुछ हिस्सा राइट ऑफ में डाल दिया जाता है, आमतौर पर निपटान के हिस्से के रूप में, जब एक खराब कर्ज को राइट ऑफ में डाल दिया जाता है. हाल ही में, वित्त मंत्री ने संसद को बताया कि भारतीय बैंकों ने वित्त वर्ष 2018 से वित्त वर्ष 2022 तक पांच वर्षों में बट्टे खाते में डाले गए 10.09 लाख करोड़ रुपये के गैर–निष्पादित ऋणों में से 13 प्रतिशत या 1.32 लाख करोड़ रुपये की वसूली करने में सफ़लता हासिल की है.
- इसमें ऋण वसूली न्यायाधिकरणों सहित सभी उपलब्ध तंत्रों से वसूली, दिवाला और दिवालियापन संहिता (आईबीसी) के तहत सुलझाए गए मामले, सरफेसी अधिनियम के तहत की गई कार्रवाई, परिसंपत्ति पुनर्निर्माण कंपनियों को गैर–निष्पादित ऋणों की बिक्री, और इसी तरह के अन्य तंत्र भी शामिल हैं.

पुनर्प्राप्ति के उपाय:

ऋण वसूली न्यायाधिकरण :

- वे ग्राहकों के साथ बैंकों और अन्य वित्तीय संस्थानों को शामिल कर ऋण वसूली की सुविधा के लिए कार्य करते हैं.

सरफेसी अधिनियम, 2002:

- यह बैंकों और अन्य वित्तीय संस्थानों को ऋण की वसूली के लिए आवासीय या वाणिज्यिक संपत्तियों (डिफ़ॉल्ट रूप से) की नीलामी करने की अनुमति देता है.
- अधिनियम गैर–निष्पादित संपत्तियों की वसूली के लिए तीन वैकल्पिक तरीके प्रदान करता है–
  1. प्रतिभूतिकरण,
  2. संपत्ति पुनर्निर्माण और
  3. न्यायालय के हस्तक्षेप के बिना सुरक्षा का प्रवर्तन.

दिवाला और दिवालियापन संहिता (आईबीसी) :

- आईबीसी का उद्देश्य समयबद्ध तरीके से निगमों, व्यक्तियों और साझेदारियों के दिवालियापन को पुनर्गठित कर उनको हल करना है.

भगोड़ा आर्थिक अपराधी अधिनियम:

- यह बैंकों को टुकड़ों में संपत्तियों को जब्त करने का अधिकार देता है, भारत ने खराब ऋण वसूली के लिए पारिस्थितिकी तंत्र को मजबूत करने में महत्वपूर्ण प्रगति की है.

- यह उन आर्थिक अपराधियों की संपत्तियों को जब्त करने या उन संपत्तियों को जब्त करने का प्रयास करता है जो भारतीय अदालतों के अधिकार क्षेत्र से बाहर रहकर अभियोजन पक्ष से बचते हैं.

नेशनल एसेट रिकंस्ट्रक्शन कंपनी लिमिटेड (बैड बैंक):

- एनएआरसीएल को कंपनी अधिनियम के तहत शामिल किया गया है और उसने परिसंपत्ति पुनर्निर्माण कंपनी (एआरसी) के रूप में लाइसेंस के लिए भारतीय रिजर्व बैंक को आवेदन किया है.
- यह योजना 500 करोड़ और उससे अधिक के खराब ऋणों के लिए एक बैड बैंक बनाने की है, जिसमें एक संपत्ति पुनर्निर्माण कंपनी (एआरसी) और एक संपत्ति प्रबंधन कंपनी (एएमसी) शामिल होगी, जो ख़राब संपत्ति का प्रबंधन और वसूली करेगी.

एनपीए कम करने के कारण:

- यदि गैर-निष्पादित परिसंपत्तियों के पिछले कुछ दशकों के सबसे निचले स्तर पर अर्थात वित्त वर्ष 2024 में 4% (क्रिसिल के अनुसार) तक गिरने की उम्मीद है, तो इसका मुख्य कारण है
  - निजी कैपेक्स में मंदी,
  - बैंक परियोजना ऋण देने से पीछे हट रहे हैं

सुधार के मौके :

- उधार देने और अंडर राइटिंग प्रैक्टिस (ऋण देने में पारदर्शिता) में अभी भी सुधार की पर्याप्त संभावना है.
- उदाहरण के लिए, कुछ बैंक अपनी सहायक कंपनियों द्वारा प्रदान की गई 'ऑपरेटिंग कम्फर्ट' के आधार पर होल्डिंग कंपनियों के लिए अपना एक्सपोजर बढ़ा रहे हैं, जो पहले से ही काफी हद तक लीवरेज्ड हैं.
- यह प्रथा पिछले चक्र में समूह-स्तरीय ऋण जोखिम को खराब परिसंपत्तियों में परिवर्तित करने वाले प्रमुख कारणों में से एक थी.

पूर्व कार्रवाई की आवश्यकता:

- नकदी प्रवाह आधारित वित्तपोषण (एक ऐसा मॉडल जहां जोखिम को समय पर निपटाना मुश्किल होता है) तीव्र गति से बढ़ रहा है.
- इन्फ्रा-बूम दिनों की तुलना में इस तरह की प्रथाएं आज कम प्रचलित हैं.
- लेकिन जैसा कि वे अगले कैपेक्स चक्र को बैंकरोलिंग करना शुरू करते हैं, बैंकों के लिए राइट-ऑफ की आवश्यकता को कम करने का सबसे अच्छा तरीका एनपीए अभिवृद्धि को शुरुआती चरण में रोकना है .
- जब ऋण एनपीए में बदलने की प्रतीक्षा करने के बजाय एसएमए (विशेष उल्लेखित खाता) स्थिति में चले जाते हैं, तो इसके लिए अधिक प्री अटेम्प्टिव कार्रवाई की आवश्यकता हो सकती है.

भविष्य :

- आरबीआई को अपनी ओर से बैंकों को व्यवस्थित आधार पर अपने ऋण राइट-ऑफ और वसूली पर अधिक पारदर्शिता प्रदर्शित करने के लिए प्रेरित करना चाहिए.
- एनपीए, बट्टे खाते में डालने और वसूलियों का सही से समय-वार विश्लेषण करना आवश्यक है, ताकि जानबूझ कर चूक करने वालों और आर्थिक चक्रों या व्यावसायिक अनिवार्यताओं के विपरीत प्रवर्तकों द्वारा धन की हेराफेरी के परिणामस्वरूप खराब ऋणों के अनुपात को समझा जा सके.
- जहां इरादतन चूक (विलफुल डिफाल्टर) के स्पष्ट प्रमाण हैं, वहां नेम और शेम नामक पद्धति का उपयोग कर गलत करने वालों के विरुद्ध एक रक्षा उपकरण के रूप में कार्य कर सकता है और हितधारकों को सतर्क भी कर सकता है.
- इसके अलावा बैंक कर्मियों द्वारा किए जा रहे सकारात्मक प्रयासों की वृहद स्तर पर प्रशंसा होनी चाहिए और उनके वसूली प्रयासों को और अधिक वैज्ञानिक स्वरूप देने और विशेष अधिकार देने की आवश्यकता है.

माधवी दत्त
शाखा प्रबन्धक
शाखा बेसा रोड

अदावाकृत खातों का सक्रियकरण

बैंकों का मूल व्यवसाय जमा लेना एवं ऋण वितरण करना होता है. बैंकों में राशि जमा करने के लिए लोगों द्वारा खाता खोला जाता है. ये बचत/चालू खातें जब दस वर्षों तक संचालित नहीं होते एवं सावधि जमा के परिपक्वता से दस वर्षों तक आहरण न होने पर ये खातें अदावाकृत खातों में परिवर्तित किये जाते हैं.

अनुभाग 26, बैंकिंग रेगुलेशन एक्ट 1949 के अनुसार बैंकों को इन खातों की जानकारी प्रति वर्ष के अंत से तीस दिन के भीतर रिजर्व बैंक को देनी होती है. यह राशि दस वर्षों या उससे अधिक होने पर तीन माह की अवधि में रिजर्व बैंक को DEAF (डिपोजिट एजुकेशन एण्ड अवेयरनेस फण्ड) में परिवर्तित होकर निधि अंतरित होती है. जिसके उपरान्त खाता धारक बैंकों के दिशानिर्देशानुसार सही क्लेम प्रकरण के माध्यम से प्राप्त कर पाता है.

वर्तमान में बैंकों एवं रिजर्व बैंक द्वारा अदावाकृत खातों के सक्रियकरण को लेकर कई जन जागरण अभियान चलाये जाने पर भी इन खातों की संख्या एवं राशि में वृद्धि पाई गई है.

लगातार बढते अदावाकृत खातों का मूल कारण अनावश्यक बचत/चालू खातों को बंद नहीं करना एवं सावधि जमा राशि को परिपक्वता के बाद भी आहरण नहीं करना पाया गया है. अधिकतर मृतक खाता धारकों के बचत/सावधि जमा खाते इस श्रेणी में आ जाते है. प्राय: जब इन खातों में नामिनी/लीगल हेयर्स (कानूनी वारिस) इस राशि का पहचान व दावा नहीं करते है.

आर्थिक रुप से सक्षम लोगों में इन खातों के प्रति अरुचि एवं अज्ञानता भी इसका एक बडा कारण है.

पिछले एक दशक 2011 से 2020 के आँकडों मे अदावाकृत खातों की संख्या एवं राशि में काफी बढत देखी गई है. वस्तुत: राशि में 29.10 प्रतिशत एवं संख्या में 24.10 प्रतिशत की वृद्धि पायी गई है. इससे यह स्पष्ट होता है कि अधिक जमा राशि वाले बचत/चालू/सावधि खातें ज्यादा संख्या में अदावाकृत खातों के रुप में समूहित हुए है जो चिन्ता का विषय है.

वर्ष 2020–21 में बारह सरकारी बैंकों, बारह पूर्व के निजी बैंकों एवं नौ नये निजी बैकों से इन खातों के आँकडें एकत्रित किये गए। जिसमें सरकारी बैंकों में 1.26 प्रतिशत अदावाकृत खातों का जमा मार्च 2021 तक खाताधारक या कानूनी वारिसों द्वारा दावा किया गया। पूर्व के निजी बैंकों में 1.22 प्रतिशत एवं नये निजी बैंकों में 0.79 प्रतिशत दावा के लिए आया। जो की कुल अदावाकृत जमा का छोटा अंश मात्र ही है.

बचत/सावधि जमा खातों के अदावाकृत खातों में परिवर्तन का मुख्य कारण खातों में नामिनी विवरण न होना, खातों में पूरा पता का न होना एवं खातों का ज्वाइंट (संयुक्त संचालन आदेश) न होना है. ऐसे में खाताधारक के बाद जमा राशि की जानकारी परिवार जनों को न होना अथवा स्वयं खाताधारक द्वारा संचालन न करना आदि से खाता निष्क्रिय हो जाता है.

तदोपरांत भी यह खाताधारक अथवा उत्तराधिकारी की जिम्मेदारी होती है कि खाते की राशि को आहरण करने या खाते को बंद करने के लिए बैंकों के दिशा निर्देशों का पालन करें जो कि बोझिल एवं समय लेने वाला हो जाता है.

वित्तीय साक्षरता एवं सही विधान की जानकारी न होना ही इस तरह की स्थिति उत्पन्न करता है.

बैंकों द्वारा संभावित समाधान:

खातों की ऐसी समूहित सूची को बढने से रोकने के लिए निम्न प्रयास किए जा सकते है.

- खाता खोलते समय ही बैंक नामिनेशन अवश्य कराये
- क्योंकि सावजनिक बैंक छोटे खाताधारकों का बैंक हैं अतः इस प्रकार उनके खातों को अदावाकृत खातों में परिवर्तित होने से रोकना बैंकों की भी जिम्मेदारी बनती है. जिसके लिए सार्थक प्रयास करना चाहिऐ

- बैंकों को क्षेत्रावार शिविर का आयोजन करना चाहिए जिसके द्वारा अदावाकृत व निष्क्रिय खातों की सूची एवं निर्देशों की जानकारी आम जनता को देनी चाहिए.
- अदावाकृत खातों की स्थिति पर निगरानी रख कर ग्राहक शिकायत निवारण प्रक्रिया के माध्यम से त्वरित निपटान करना चाहिए.
- बी. सी. (व्यापार संवाददाता) की मदद से भी इन खाताधारकों या उनके कानून वारिसों से सम्पर्क कर खातों का पुनर्संचालन करवाना चाहिए.
- अल्प राशि वाले जमा खातों को बैंक द्वारा कानूनन उत्तराधिकारी का सही पहचान कर कम से कम काग़जी कार्यवाही से एवं सुलभ सरल प्रक्रिया द्वारा निपटान करना चाहिए ताकि बैंकों एवं खाताधारकों का दोनों का समय एवं शुल्क बचत किया जा सके.

रिजर्व बैंक द्वारा समय-समय पर बैंकों को दिशानिर्देश दिये जाते हैं एवं जनता को जागरुक करने हेतु विभिन्न अभियान चलाये जाते हैं. टी. वी., रेडियो एवं सोशल मीडिया के माध्यम से इन खातों के पुन: संचालन करने एवं प्रक्रिया की भी जानकारी दी जा रही है. जिसके अन्तर्गत अपने के. वाय. सी., मोबाइल संख्या, ई-मेल अपडेट एवं नामिनी अपाइन्ट करना इत्यादि की जानकारी दी जा रही है. इनके द्वारा साथ ही खाताधारक अपने मोबाइल संख्या, ई-मेल एवं पता आदि बदलने पर स्वयं की जिम्मेदारी मानते हुए अनिवार्यत: इन्हे अपने खाता में अद्यतन करवाना चहिए, इसमें खाताधारक की ही भलाई होती है. समय समय आने वाले बैंकों के अपडेट्स एवं सुविधाएँ तुरंत प्राप्त की जा सकतीं हैं.

रिजर्व बैंक द्वारा कुछ विवरण सुधार हेतु अदावाकृत खातों के आँकडों में सलग्न किया जा सकता है जिससे इन खातों की सही स्थिति को परखा जा सके एवं उन पर योजनाबद्ध तरीके से कार्य किया जा सके.

1. जनसंख्या वार (ग्रामीण/अर्ध-शहरी/शहरी/मेट्रो) अदावाकृत खातों के आँकडें बैंकों से लिए जायें.
2. समय-समय पर अधिकारियों द्वारा बैंकों के निरीक्षण के दौरान इन खातों की स्थिति का अवलोकन करें.

रिजर्व बैंक के निर्देशानुसार लोगों की जमा राशि डी. ई. ए. एफ. में जाने के बाद भी बैंक सही वारिसों को क्लेम प्रक्रिया के जरिए सौपने को बाध्य है. अत: रिजर्व बैंक के पास जमा अदावाकृत खातों की राशि को पुन: खाता धारकों तक लाने के लिए बैंकों के सतत प्रयास एवं खाताधारकों की साझा जिम्मेदारी होनी आवश्यक है.

इन अदावाकृत खातों के समूहित सूची के लाभ का इस प्रकार विश्लेषण किया जा सकता है:
दस या उससे अधिक वर्षों के लिए खाते का संचालन (लेन-देन) न होने पर रिजर्व बैंक के निर्देशानुसार अदावाकृत खाता माना जाता है. हालांकि ये अदावाकृत खाते कानूनी सीमाओं से मुक्त है. इसका मतलब है कि लाभार्थी किसी भी समय धनराशि निकालने के लिए बैंक में अपने पहचान पत्रों के साथ में सम्पर्क कर राशि का आहरण कर सकता है. जिनके भी दिशानिर्देश रिज़र्व बैंक द्वारा निर्धारित किए गए है.

खातों को अदावाकृत समूह में वर्गीकृत करने का लक्ष्य धोखाधडी के जोखिम को कम करना है. एक बार इस प्रकार वर्गीकृत खातों की पहचान हो जाने पर संबंधित ऑफिसर को इन खातों की संख्या बढने के बारे में सूचित किया जाता है. यह उन्हे धोखाधडी गतिविधियों और संदिग्ध लेन-देन पर नजर रखने के लिए, इन खातों के माध्यम से किये गए लेन-देन पर अतिरिक्त ध्यान देने में सक्षम बनाता है. खातों के अदावाकृत होने पर खाते में अन्य व्यक्ति विशेष द्वारा लेन-देन व पैसों की धोखाधडी से सुरक्षित रखा जाता है.

चूँकि बैंक कर्मचारियों के लिए खाताधारक के दस्तावेज़ एवं नमूना हस्ताक्षर प्राप्त करना आसान होता है. बेइमान कर्मचारी इसका उपयोग निकासी पर्चियों द्वारा पैसे निकालने के लिए कर सकता है. अत: इस प्रकार अदावाकृत खातों के समूह ऐसी धोखाधडी से बच जाते है.

अपने खातों को अदावाकृत होने से बचाने के लिए एक मात्र मानदंड उपयोगकर्ता प्रेरित लेन–देन है. जिन्हे निम्नानुसार समझा जा सकता है.

1. अगर अलग–अलग बैंकों में कई अनावश्यक खाते खुले हुए है तो उन्हें बंद किया जा सकता है. एवं जो खाते उपयोग में रखने है उनके पासबुक, ए.टी.एम. एवं चेकबुक इत्यादि संभाल कर रखा जाये.
2. साथ ही नकदी निकालना, नेट बैंकिंग एवं मोबाइल एप का उपयोग करके राशि अंतरण करना या चेक भुगतान करने से खाते मे निरंतर संचालन माना जाता है.
3. सावधि जमा करने पर उसकी बैंक रसीद पर हर बार नवीनीकरण की जानकारी रखना एवं हर वर्ष व्याज प्रमाण पत्र रखने से इसकी अवधि की सही जानकारी रहती है. और समयावधि होने पर इसका आहरण भी किया जा सकता है.
4. पुराने खातों में पासबुक अनिवार्यत: दिया ही जाता था, ऐसे में बैंक के अन्य कोई भी दस्तावेज चेक बुक, ए.टी.एम., FD रसीद आदि घरों की अलमारी में मिले तो इसकी पूरी जानकारी बैक में जाकर लेनी चाहिए.
5. खातों में मोबाइल नम्बर/घर का पता या ई–मेल डला हो तो वर्तमान में चल रहे अभियान के अन्तर्गत बैंक कर्मचारी स्वयं ही इन खाता के खाताधारक का पता लगाने की मुहिम चला कर सम्पर्क करने की कोशिश कर रहे हैं.

इन अदावाकृत खातों के पता चलने पर स्वयं खाताधारक अपने पैन कार्ड, आधार कार्ड साथ ही बैंक खाते के दस्तावेज लेकर स्वयं बैंक मे उपस्थित हो सकता है और पूरी जानकारी ले सकता है. बैंक खाते को पुन: सक्रिय करने या बंद कर पूरी राशि आहरण करने से पूर्व ग्राहक की साख स्त्यापित करती है.

तदोपरांत उतनी राशि बैंक के नॉमिनल खाते से निकाल कर खाताधारक को सौंप दी जाती है. तत्पश्चात इसका क्लेम रिज़र्व बैंक से (जमा राशि वापस लेने हेतु) किया जाता है. साथ ही इसमें बचत खाते के अनुरुप ब्याज देने का भी प्रावधान होता है.

यदि खाताधारक के कानूनी वारिस इन पर दावा करते हैं तो उसी नियम के निर्देशानुसार उत्तराधिकारी का के. वाय. सी., खाताधारक का मृत्यु प्रमाण पत्र या अन्य कानूनी दस्तावेज, गवाह और बैंक के उपलब्ध पासबुक या अन्य दस्तावेज को लेकर बैंक में सम्पर्क करना होता है. इस प्रक्रिया में खाताधारक हो या कानूनी वारिस, उन्हें व्यक्तिगत रुप से उपस्थित होना होता है.

इस प्रकार खाताधारक/उत्तराधिकारी एवं बैंकों के परस्पर सहयोग से इन खातों की सूची कम/छोटी की जा सकती है. एवं राशि को सही हकदार तक पहुँचाया एवं सौपा जा सकता है.

रिज़र्व बैंक के हालिया आदेश में उल्लेख किया गया कि बैंकों को सभी खातों की सालाना समीक्षा करनी चाहिए. उन्हें एक लिखित संप्रेषण भेजना होगा जिनमें एक वर्ष से अधिक समय तक खाते का उपयोग न करने का कारण पूछा जाएगा.

अंतिम सुझाव:
लंबे समय तक निष्क्रिय खाते अदावाकृत खातों में परिवर्तित हो जाते हैं जिससे वह राशि न खाते में रहती है न किसी लेन–देन के उपयोग मे आती है. वरण उस राशि को बिना बैंक में उपस्थित होए निकाला भी नहीं जा सकता है. अतः जिन खातों की आवश्यकता न हो उन्हे बंद करना ही खाताधारक के हित में होता है.

साथ ही अगर अब तक परिवार जनों के ऐसे कोई खातों की जानकारी हुई हो तो तुरंत बैंक में उन दस्तावेजों को लेकर मिले जिससे इन खातो को कम किया जा सके. मिशन मोड पर चल रहे बैंक के इस अभियान को जिम्मेदारी से करें एवं लाभ उठायें.

एम पुष्पलता
वरिष्ठ प्रबंधक
सेन्ट्रल बैंक ऑफ इंडिया

राइट ऑफ खातों में वसूली

भारतीय रिज़र्व बैंक के दिशानिर्देशों और बैंक के बोर्ड द्वारा अनुमोदित नीति के अनुसार अनर्जक अस्तियों (एनपीए), जिसमे अन्य बातों के साथ-साथ वैसे एनपीए शामिल हैं, जिनके चार वर्ष पूरे होने पर, पूर्ण प्रावधान किया गया हो, को बट्टे खाते (राइट ऑफ) में डालकर सम्बंधित बैंक के बैलेंस शीट से हटा दिया जाता है. आरबीआई के दिशानिर्देशों और अपने बैंक के बोर्ड द्वारा अनुमोदित नीतियों के अनुसार बैंक अपने बैलेंस शीट को साफ़ करके, कर-लाभ प्राप्त करने और कैपिटल ऑप्टिमाइजेशन करने के लिए नियमित रूप से राइट-ऑफ खातों का अवलोकन, विश्लेषण और मूल्यांकन करते हैं.

भारतीय संसद के दसवे सत्र में, माननीय वित्त मंत्री, श्रीमती निर्मला सीतारमन, ने एक तारांकित प्रश्न के जवाब में 19 दिसम्बर 2022 को बताया था की:

भारतीय रिज़र्व बैंक से प्राप्त सूचना के अनुसार अनुसूचित वाणिज्यिक बैंकों ने पिछले पांच वर्षों के दौरान 10,09,511 करोड़ रुपए (10,09,511) की राशि बट्टे खाते (राइट ऑफ) में डाली है. आरबीआई के आंकड़ों के अनुसार, सार्वजनिक क्षेत्र के बैंकों ने विगत पांच वित्तीय वर्षों के दौरान बट्टे खाते (राइट ऑफ) में डाले गए ऋणों में से 1,03,045 करोड़ रुपये की वसूली सहित कूल 4,80,111 करोड़ रुपए की वसूली की है.

आरबीआई के आंकड़ों के अनुसार, प्रमुख सरकारी बैंकों के विवरण, क्रमागत रूप में कुछ इस प्रकार है:

राशी करोड़ रुपए में

बैंक	वित्तीय वर्ष २०१७-२०१८	वित्तीय वर्ष २०१८-२०१९	वित्तीय वर्ष २०१९-२०२०	वित्तीय वर्ष २०२०-२०२१	वित्तीय वर्ष २०२१-२०२२	कूल
भारतीय स्टेट बैंक	३९१५१	५८९०५	५२३६२	३४४०२	१९६६६	२०४४८६
पंजाब नेशनल बैंक	७४०७	१२२१५३	१३३६५			
ओरिएंटल बैंक ऑफ कॉमर्स	६३५७	६४५७	३३५१	१५८७७	१८३१२	२०२३३९
यूनाइटेड बैंक ऑफ इंडिया	१८६७	५३६५	१७२८			
यूनियन बैंक ऑफ इंडिया	३४७७	७७७१	८४१७			
आंध्रा बैंक	१६६६	२२८०	४१९५	१६९८३	१९४८४	८२३०४
कॉर्पोरेशन बैंक	८२२८	५९८९	३८१४			
बैंक ऑफ बड़ोदा	४९४८	१३१०२				
देना बैंक	६६१	४६७२	१५९१२	१४७८२	१७९६७	७५१०१
विजया बैंक	१५३९	१५१८				
केनरा बैंक	८३१०	१४२६७	७४९८	७६४२	८२१०	६००३६
सिंडिकेट बैंक	२४००	६७७५	४९३४			
बैंक ऑफ इंडिया	८९७६	७४०५	७६१८	८८१५	१०४४३	४३२५७
इंडियन बैंक	१६०६	२८७२	३०३२	८३७१	८३४७	४१२०२
इलाहाबाद बैंक	३६३५	४३१९	९१२०			
इंडियन ओवरसीज बैंक	६९०८	७७९४	१६४०५	४६१८	३७६९	३९४९४
यूको बैंक	२७३५	४४२०	१२४७९	९४१०	३८५१	३२८९५
सेंट्रल बैंक ऑफ इंडिया	२,९२४	१०,३७५	४,१६९	५९९२	१२३६	२४६९६
बैंक ऑफ महाराष्ट्र	२४६०	५१२७	५६९८	४९३१	३११८	२१३३४
पंजाब एंड सिंध बैंक	४६०	१६३५	१७८१	७१	११३४	५७८१

बैंकों के पास वसूली के विकल्प

इन आंकड़ो को देखने के बाद ये तो समझ में आता है की, राइट-ऑफ खातों में डाली गई राशि अगर वसूल हो जाये, तो वो किसी दुर्लभ खजाने से कम नहीं है, जो की किसी भी बैंक/ बैंकिंग सेक्टर की दशा एवं दिशा दोनों बदल सकता है. परन्तु गौर करने वाली बात ये है की, वर्तमान में बैंकों के पास क्या विकल्प है और वो कितने कारगर है?

बैंकों के पास विभिन्न वसूली तंत्र, जो उपलब्ध हैं, वो निम्नलिखित हैं:

I. सिविल न्यायालय में वाद दायर करके:

सरफेसी अधिनियम/ विभिन्न न्यायाधिकरण/ अधिनियम, एक लाख रुपये से अधिक की बकाया राशि पे लागु होते है, इसलिए व्यावहारिक तौर पे, बैंकों/ वित्तीय संस्थान, सिविल न्यायालय में निम्नलिखित बकाया राशि की वसूली के लिए वाद दायर करते है:

- एक लाख रुपये से कम की बकाया राशि, की वसूली के लिए. (सेक्योर्ड और अनसेक्योर्ड - दोनों तरह के ऋण के लिए)
- बीस लाख रुपये से कम की बकाया राशि, की वसूली के लिए. (अनसेक्योर्ड ऋण के लिए)

यहाँ लोक अदालतें, अपनी सुलभ एवं सस्ती न्यायिक प्रणाली के चलते, एक उपयोगी माध्यम साबित हुई है. इसमें बैंक 20 लाख रुपए से कम राशी के ऋण की वसूली के लिए जाते है.

ii. वित्तीय आस्तियों का प्रतिभूतिकरण और पुनर्गठन और प्रतिभूति हित का प्रवर्तन अधिनियम, 2002 (सरफेसी एक्ट, 2002):

सरफेसी अधिनियम 2002, बैंकों और वित्तीय संस्थानों को किसी भी हस्तक्षेप के बिना उधारकर्ता/गारंटर की सुरक्षित संपत्तियों के खिलाफ कार्रवाई करने का अधिकार देती है. इस अधिनियम के अंतर्गत कार्यवाही के लिए बकाया राशि एक लाख रुपये से अधिक होनी चाहिए.

किसी भी पीड़ित देनदार/उधारकर्ता के पास सरफेसी अधिनियम के तहत कार्रवाई के खिलाफ, ऋण वसूली न्यायाधिकरण (डीआरटी) में अपील दायर करने का सहारा है और डीआरटी के फैसले के खिलाफ अपील करने के लिए आगे ऋण वसूली अपीलीय न्यायाधिकरण (डीआरएटी) में विकल्प उपलब्ध है.

iii. ऋण वसूली न्यायाधिकरण/ ऋण वसूली अपीलीय न्यायाधिकरण में वाद दायर करके (डीआरटी/ डीआरएटी कोर्ट):

भारतीय बैंक और वित्तीय संस्थान लंबे समय से डिफॉल्टरों से कर्ज वसूलने और प्रतिभूतियों को लागू करने के लिए संघर्ष कर रहे थे. चूंकि इस तरह की वसूली से संबंधित प्रक्रिया अनियमित और बेहद बोझिल थी, इसलिए 1991 की नरसिम्हम समिति ने ऐसी प्रक्रियाओं को सुव्यवस्थित करने के लिए डीआरटी और डीआरएटी जैसे विशेष न्यायाधिकरणों की स्थापना की सिफारिश की थी. समिति की सिफारिश के कारण बैंकों और वित्तीय संस्थानों के लिए ऋण वसूली अधिनियम (आरडीडीबीएफआई) 1993 लागू हुआ, जिससे डीआरटी और डीआरएटी को ऋण वसूली मामलों पर निर्णय लेने का अधिकार प्राप्त होता है. हमारे पास देश में वर्तमान में 39 डीआरटी और 5 डीआरएटी कार्य कर रहे हैं.

इस कानून की मुख्य विशेषताएं इस प्रकार हैं:

- 20 लाख रुपये से अधिक के ऋण की वसूली के लिए बैंक, डीआरटी में वाद दायर कर सकती है.
- डीआरटी व्यापक आदेश पारित करने के लिए पूरी तरह से सशक्त हैं और पूर्ण न्याय प्रदान करने के लिए सिविल प्रक्रिया संहिता से परे भी जा सकते हैं.
- हालाँकि डीआरटी, ऋणदाताओं की ओर से क्षति या सेवाओं की कमी या अनुबंध के उल्लंघन या आपराधिक लापरवाही के दावों की सुनवाई नहीं कर सकता है.
- सुप्रीम कोर्ट और हाई कोर्ट के अलावा देश में किसी भी अदालत के पास इस मामले पर कोई अधिकार क्षेत्र है. सुप्रीम कोर्ट और हाई कोर्ट, भी केवल संविधान के अनुच्छेद 226 और 227 के तहत सिमित अधिकार क्षेत्र है.
- डीआरटी में 6 महीने के भीतर मामलों को निष्पादित करने का प्रावधान है. सरफेसी अधिनियम के मामले में, मामलों को निपटाने की समय अवधि 60 दिन से 4 महीने तक है.
- डीआरटी द्वारा पारित आदेशों के खिलाफ अपील, 45 दिनों के भीतर डीआरएटी के समक्ष दायर की जा सकती है, इसके लिए पहले, पीड़ित पक्ष को निर्धारित राशि का 75% जमा करना होता है.
- अपीलीय न्यायाधिकरण (डीआरएटी) के समक्ष अपीलों का निपटारा, प्राप्ति तिथि से 6 महीने के भीतर किया जाएगा.

iv. दिवाला और शोधन अक्षमता संहिता, 2016 के अंतर्गत राष्ट्रीय कंपनी विधि अधिकरण में मामला दायर करके, (आई बी सी अधिनियम/ एन सी एल टी):

भारत में, ऋण डिफाल्टरों से निपटने के लिए, कानूनी और संस्थागत तंत्र, वैश्विक मानकों के अनुरूप नहीं थे. लेनदारों द्वारा वसूली कार्रवाई या तो अनुबंध अधिनियम के माध्यम से या विशेष कानूनों जैसे आरडीडीबीएफआई अधिनियम 1993 अथवा सारफेसी अधिनियम 2002 के माध्यम से की गई, परन्तु इसके इच्छित परिणाम नहीं आये. इसी तरह, बीमार औद्योगिक कंपनी (विशेष प्रावधान) अधिनियम, 1985 और कंपनी अधिनियम, 1956 (के समापन सम्बन्धी प्रावधानों) के माध्यम से की गई कार्रवाई, न तो उधारदाताओं के लिए वसूली में सहायता करने में सक्षम हो पाई और न ही फर्मों के पुनर्गठन में सहायता करने में सक्षम हुई. व्यक्तिगत दिवाला से संबंधित कानून, राष्ट्रपति नगर दिवाला अधिनियम, 1909 और प्रांतीय दिवाला अधिनियम 1920, भी लगभग एक सदी पुरानी हो चुकी थी.

इस कानून का उद्देश्य उद्यमशीलता, ऋण की उपलब्धता को बढ़ावा देना और समयबद्ध तरीके से कॉर्पोरेट व्यक्तियों, साझेदारी फर्मों और व्यक्तियों के पुनर्गठन और दिवालियापन समाधान से संबंधित कानूनों को समेकित और संशोधित करके सभी हितधारकों के हितों को संतुलित करना था. इसका एक उद्देश्य वर्तमान के कई कानूनों को एक ही कानून में समेकित करना था. इस तरह का एकीकरण, कानून में अधिक स्पष्टता प्रदान करता और व्यवसाय की विफलता या ऋण का भुगतान करने में असमर्थता से प्रभावित विभिन्न हितधारकों के लिए सुसंगत और सुसंगत प्रावधानों को लागू करने की सुविधा प्रदान करता.

इस कानून की मुख्य विशेषताएं इस प्रकार हैं:

- इस अधिनियम के चार संस्थागत बुनियादी स्तंभ है:
  - पहला स्तंभ विनियमित व्यक्तियों का एक वर्ग है, 'इन्सोल्वेंसी प्रोफेशनल'.
  - दूसरा स्तंभ 'सूचनाओ की उपयोगिताओं' का एक नया उद्योग है. ये ऋणदाताओं और ऋण देने की शर्तों के बारे में तथ्यों को इलेक्ट्रॉनिक डेटाबेस में संग्रहीत करेंगे. इससे डिफॉल्ट होने पर होने वाली देरी और तथ्यों को लेकर विवाद खत्म हो जाएगा.
  - तीसरा स्तंभ निर्णय लेने में है. एन.सी.एल.टी वह मंच होगा, जहां फर्म के दिवालियेपन की सुनवाई की जाएगी और डी.आर.टी वह मंच होगा जहां व्यक्तिगत दिवालियेपन की सुनवाई की जाएगी. इन संस्थानों को उनके अपीलीय निकायों अर्थात एन.सी.एल.ए.टी और डी.आर.ए.टी के साथ पर्याप्त रूप से मजबूत किया गया ताकि दिवालियेपन प्रक्रिया की विश्व स्तरीय कार्यप्रणाली को प्राप्त किया जा सके.
  - चौथा स्तंभ एक नियामक है, 'भारतीय दिवाला और दिवालियापन बोर्ड'. यह निकाय इन्सॉल्वेंसी प्रोफेशनल, इन्सॉल्वेंसी प्रोफेशनल एजेंसियों और सूचना उपयोगिताओं पर नियामक निगरानी रखेगा.
- इस कानून का मूल विचार यह है कि जब कोई कंपनी अपने ऋण पर डिफाल्ट करती है, तो नियंत्रण शेयरधारकों / प्रमोटरों से लेकर, ऋणदाताओं की एक समिति के पास चला जाता है, जिसके पास कंपनी को पुनर्जीवित करने या इसे अपने अधीन लेने के बारे में विभिन्न खिलाड़ियों के प्रस्तावों का मूल्यांकन करने के लिए 180 दिन होते हैं.
- यह कानून सीमा पार दिवालियापन से निपटने में भी सक्षम है.

यह अधिनियम, भारत को अपेक्षाकृत कमज़ोर दिवालिया व्यवस्थाओं से निकालकर दुनिया की सर्वश्रेष्ठ दिवालिया व्यवस्थाओं में से एक बनाने के लिए लाया गया था. यह कॉर्पोरेट बांड बाजार के विकास की नींव रखता, जो भविष्य की बुनियादी इन्फ्रास्ट्रक्चर परियोजनाओं को वित्तपोषित करता.

v. बातचीत द्वारा निपटान/ समझौते के माध्यम से (ओ.टी.एस स्कीम/ सेटलमेंट स्कीम):

आरबीआई के निर्देशों के अनुसार, सभी बैंकों के पास एक ऐसी नीति होनी चाहिए, जिसमें अन्य बातों के साथ-साथ एनपीए का बातचीत के जरिए/समझौते से निपटारा शामिल हो. ये ओ.टी.एस योजनाएं बैंकों की बोर्ड-अनुमोदित नीतियों के अनुसरण में होती हैं, और आम तौर पर कृषि, सूक्ष्म लघु और मध्यम उद्यम (एमएसएमई), कमजोर वर्गों और शिक्षा ऋण जैसे क्षेत्रों की ओर उन्मुख होती हैं.

इसके अलावा, जनवरी 2018 में सरकार द्वारा घोषित पी.एस.बी सुधार एजेंडा के तहत, पी.एस.बी बैंकों ने स्वच्छ कंसोर्टियम ऋण व्यवस्था एवं कठोर वसूली के लिए, स्ट्रेस्ड एसेट मैनेजमेंट वर्टिकल की स्थापना की जोकि 250 करोड़ रुपये से ऊपर के ऋणों की वसूली देखता है.

vi. अनर्जक आस्तियों की बिक्री करके (ए.आर.सी/ एन.ए.आर.सी.एल-आई.आर.डी.सी.एल):

क्रिलिक (सि.र.आई.एल.आई.सी) डेटा के अनुसार, कॉर्पोरेट कंपनी उधारकर्ताओं की एनपीए के रूप में वर्गीकृत की गई बकाया राशि 31.3.2023 तक 1,03,975 करोड़ या उससे अधिक थी (यह सिर्फ 1,000 करोड़ रुपये या उससे अधिक के ऋण के मामलों में था).

- मौजूदा ए.आर.सी व्यवस्था (वर्तमान में 28 से अधिक) – छोटे मूल्य के ऋणों के समाधान में सहायक रहे हैं.
- पुराने एनपीए (राइट-ऑफ) के बड़े भंडार को देखते हुए, अतिरिक्त विकल्पों की आवश्यकता थी और केंद्रीय

बजट में घोषित एन.ए.आर.सी.एल–आई.आर.डी.सी.एल संरचना यह पहल है.

- नेशनल एसेट रिकंस्ट्रक्शन कंपनी लिमिटेड की स्थापना एक परिसंपत्ति पुनर्निर्माण कंपनी के रूप में की गई है, जिसका उद्देश्य प्रत्येक 500 करोड़ रुपये से अधिक की तनावग्रस्त संपत्तियों का समाधान करना है. सरकार ने तनावग्रस्त ऋण परिसंपत्तियों को प्राप्त करने के लिए ऋण देने वाले संस्थानों को एन.ए.आर.सी.एल द्वारा जारी सुरक्षा रसीदों के समर्थन में 30,600 करोड़ रुपये तक की गारंटी को भी मंजूरी दे दी है.
- एनएआरसीएल ने आरबीआई के मौजूदा नियमों के तहत चरणबद्ध तरीके से लगभग 2 लाख करोड़ रु. की तनावग्रस्त संपत्ति हासिल करने का प्रस्ताव रखा है. इसका इरादा, इन्हें 15% नकद और 85% सुरक्षा रसीदों (एसआर) के माध्यम से हासिल करने का है.

परन्तु, अगर उपरोक्त विकल्पों (ए.आर.सी/ एन.ए.आर.सी.एल–आई.आर.डी.सी.एल को छोड़कर) का विश्लेषण किया जाये तो, इन सारे विकल्पों के रहते हुए भी बैंकिंग सेक्टर मात्र 11–15% (अनुमानित) ही वसूली कर पाया है. इसके कई मुख्य कारण है, जैसे, न्यायिक व्यवस्था की जटिलताये, बड़े–बड़े डीफाल्टरो कें वाद पे 85–95% (हेअरकट) पे एन.सि.एल.टी से आदेश पारित होना, वसूली में ऋणदाताओं के अनुपातहीन संसाधनों का उपयोग होना, ज्यादातर मामलों में न्यायालयों द्वारा डीफाल्टरों के प्रति नरम रवैय्या/ रियायती रुख अपनाना, कई लोन खातों में संपार्श्विक सुरक्षा (कोलैटरल सिक्यूरिटी) का न होना, कृषि ऋणों के प्रति सरकार की उदासीनता इत्यादि है.

आरबीआई के आंकड़ों के अनुसार, वर्ष 2017 तक, इन विकल्पों के द्वारा, वसूली की स्थिति कुछ इस प्रकार थी:

(राशी 'करोडो में)

वित्तीय-वर्ष	क्र. सं	वसूली के माध्यम	लोक अदालत	डी.आर.टी	सारफेसी एक्ट	कूल
2012-13	1	दायर मामले	८४०६९१	१३४०८	१९०५३७	१०४४६३६
	2	बकाया राशि	६६००	३१०००	६८१००	१०५७००
	3	वसूली गई राशि*	४००	४४००	१८५००	२३३००
	4	वसूली (% में - 2 के अनुपात में 3)	६	१४	२७	२२
2013-14	1	दायर मामले	१६३६९५७	२८२५८	१९४७०७	१८५९९२२
	2	बकाया राशि	२३२००	५५३००	९५३००	१७३८००
	3	वसूली गई राशि*	१४००	५३००	२५३००	३२०००
	4	वसूली (% में - 2 के अनुपात में 3)	६	१०	२७	१८
2014-15	1	दायर मामले	२९५८३१३	२२००४	१७५३५५	३१५५६७२
	2	बकाया राशि	३१०००	६०४००	१५६८००	२४८२००
	3	वसूली गई राशि*	१०००	४२००	२५६००	३०८००
	4	वसूली (% में - 2 के अनुपात में 3)	३	७	१६	१२
2015-16	1	दायर मामले	४४५६६३४	२४५३७	१७३५८२	४६५४७५३
	2	बकाया राशि	७२०००	६९३००	८०१००	२२१४००
	3	वसूली गई राशि*	३२००	६४००	१३२००	२२८००
	4	वसूली (% में - 2 के अनुपात में 3)	४	९	१७	१०
2016-17	1	दायर मामले	२१५२८९५	२८९०२	८००७६	२२६१८७३
	2	बकाया राशि	१०५७८७	६७०८९	११३१००	२८५९७६
	3	वसूली गई राशि*	३८०३	१६३९३	७७५८	२७९५४
	4	वसूली (% में - 2 के अनुपात में 3)	४	२४	७	१०

नोट्स : 1. *: वसूली गई राशि, वर्तमान एवं पिछले वर्षों में दायर की गई मुकदमो/ वादों की सम्मिलित तौर पे है।

वैश्विक अर्थव्यवस्थाओं का इसपर रुख

यूरोपियन यूनियन, में उसके नियंत्रक (इ.बी.ए) ने राइट–ऑफ को लेकर कोई समय–सारिणी/ नियमावली नहीं बना रखी है. हालाँकि कुछेक देशों (पुर्तगाल, आयरलैंड, स्लोवानिया, स्पेन इत्यादि) द्वारा, क्षेत्रीय स्तर पे कुछ दिशा–निर्देश पारित किये गए हैं. वहां के नियमानुसार, असुरक्षित ऋणों के लिए दो साल के बाद एवं सुरक्षित ऋणों के लिए सात साल के बाद, पूरी तरह से प्रोविजनिंग होनी चाहिए.

अमेरिका, लैटिन अमेरिकी देशों में, ऋण को उसी महीने राइट–ऑफ कर दिया जाता है, जब उसे लॉस कैटेगरी में रखा जाता है अथवा उसे अप्राप्य मान लिया जाता है.

कुछ देशों में बट्टे खाते में डालने के लिए समय सीमा सात से 24 महीने तक निर्धारित की गई है, जो कभी–कभी ऋण की मूल परिपक्वता पर निर्भर करती है.

राइट–ऑफ खातों और इसके दुस्प्रभाव से निपटने के लिए कुछ अन्य सुझाव:

1. भारतीय रिज़र्व बैंक द्वारा लाई जा रही अपेक्षित क्रेडिट हानि दृष्टिकोण (एक्सपेक्टेड क्रेडिट लोस एप्रोच) का ठोस अनुपालन एवं क्रियांन्वयन. आरबीआई द्वारा प्रारंभिक चर्चा से लगता है की संभवतः ऋण देते समय ही उसके राइट–ऑफ में जाने की सम्भावना को देखते हुए उचित प्रोविज़निंग कर ली जाएगी. अगर इसका उचित अनुपालन एवं क्रियांन्वयन किया गया तो शायद भविष्य में ये समस्या न रहे.
2. कई ऋण खातों में पूरी तरह से प्रोविज़निंग सिर्फ इस कारण से नहीं होती है, क्यूंकि, उसमे कोलैटरल सिक्यूरिटी अंकित रहती है. यहाँ गौर करने वाली बात ये है की, ज्यादातर मामलों में कोलैटरल सिक्यूरिटी का मूल्य अपने वास्तविकता से परे होता है, जिसके कारण बैंकों को मजबूरन ज्यादा नुकसान उठाना पड़ता है.

   भारतीय रिज़र्व बैंक को कुछ ऐसी व्यवस्था लानी चाहिए जिससे की, एक नियत समय के बाद (जैसे, पांच अथवा सात वर्ष) सभी ऋण खातों में शत–प्रतिशत प्रोविज़निंग लगे, और उसके बाद उसे एसेट रिकंस्ट्रक्शन कम्पनीज (एआरसी) को बेच दिया जाये.

   इस प्रक्रिया से न सिर्फ बैंकों की बैलेंस शीट समय–समय पे साफ़ होती रहेगी, बल्कि एसेट रिकंस्ट्रक्शन कम्पनीज (एआरसी) की वर्तमान उदासीनता भी दूर हो सकेगी. वर्तमान में एसेट रिकंस्ट्रक्शन कम्पनीज (एआरसी) बैंकों के एनपीए/ राइट–ऑफ खातों में दिलचस्पी इसलिए नहीं दिखाते है, क्यूंकि उसमें वसूली की सम्भावना नगण्य होती है. अगर इन एसेट रिकंस्ट्रक्शन कम्पनीज (एआरसी) को पांच अथवा सात वर्ष बाद सभी ऋण खाते, दे दिए जायेंगे, तो वो मुनाफे में भी रहेंगी और ग्राहक/ अर्थव्यवस्था को भी अनुशासित रखेंगी.

वर्तमान घटनाक्रम और भारतीय अर्थव्यवस्था पर इसका प्रभाव

राइट–ऑफ खातों का सबसे बड़ा असर, भारत सरकार के राजस्व पे पड़ता है, जोंकी, अंततः कर–दाता की ज़ेब से जाता हैं. पर बैंकों पे इसका असर, उनके पूंजी में गिरावट के तौर पे देखा जाता है. यही कारण था की, जब भारत सरकार ने बेसल नॉर्म्स के तहत पुनर्पूंजीकरण (री–कैपिटालैज़सन) की बात की, तो सबसे पहले बैंकों ने अपनी बैलेंस शीट को साफ़ करने की प्रक्रिया शुरू की, अन्यथा पुनर्पूंजीकरण करने के बाद भी बैंकों की स्थिति सुदृढ़ नहीं हो सकती थी.

राइट–ऑफ खातों का दूसरा नकारात्मक प्रभाव, विभिन्न दरों पे पड़ता है, जैसे: ऋण दर जो की महंगे होते चले जाते हैं, और जमा दर जो कम होते चले जाते हैं. इसलिए ये महत्वपूर्ण है, की राइट ऑफ खातों में वसूली, ठोस एवं कारगर तरीके से की जाये.

विभिन्न मिडिया रिपोर्टों के अनुसार, मई 2023 में, वर्तमान सरकार द्वारा भी इस विषय (राइट ऑफ खातों की वसूली) पर चिंता जाहिर की गई है, एवं सभी बैंकों को वसूली दर, वर्तमान के 11–15% से बढ़ा कर 40% तक करने का निर्देश दिया गया है.

तदनुसार, भारतीय रिज़र्व बैंक ने जून 2023, में तकनीक राइट–ऑफ और समझौता के प्रारूप (फ्रेमवर्क फॉर कोम्प्रोमाईज़ सेटलमेंट एंड टेक्निकल राइट–ऑफ) में भी कुछ परिवर्तन किये हैं.

हालाँकि यहाँ ये ध्यान देने वाली बात है, की इससे ग्राहक/ उधारकर्ता को किसी किस्म की राहत नहीं मिलती है, अपितु, बट्टे खाते में डाले गए ऋणों के उधारकर्ता, फिर भी बकाया राशी के भुगतान के लिए उत्तरदायी बने रहते हैं और बट्टे खाते में डाले गए ऋण खातों के विरुद्ध बकाया राशि की वसूली जारी रहती है.

भारतीय रिज़र्व बैंक एवं भारत सरकार की नीतियों से यह साफ़ तौर पे परिलिक्षित होता है की, वो बट्टे खाते (राइट ऑफ खातों) में वसूली को ले के सजग है, एवं वो भारतीय अर्थव्यवस्था की मजबूती को इस कारण कमजोर नहीं होने देंगे.

श्री विवेक मलिक
सहायक प्रबंधक
सेन्ट्रल बैंक ऑफ इंडिया

बैंकिंग में साइबर अपराध

प्रस्तावना–

मानव मस्तिष्क की थाह पाना सर्वथा दुष्कर कार्य है. कौन, कब, कैसे, क्या आचरण कर बैठे इसका अंदाजा सहज नहीं होता. अपराध को हम दो नजरिए से देख सकते है. ये जानते हुए भी कि अपराध तो अपराध है. भूख के लिए अपराध करना और अपराध की भूख होना ये दोनों विभिन्न पहलू है. जब अभाव/ मजबूरी अथवा अत्यंत जरूरी की स्थिति में कोई भी व्यक्ति चोरी य उठाईगिरी अथवा धोखाधड़ी के माध्यम से इन आवश्यकताओं / आभावों की पूर्ति का प्रयास करता है और कभी – कभी पश्चाताप/ आत्मग्लानि या आत्मप्रकाश अथवा किसी प्रेरक से प्रभावित हो वह पूर्णतः बदल भी जाता है. लेकिन दूसरी ओर एक बार इस दिशा में कदम उठा लेने के पश्चात् भविष्य में यह आदत का रूप ले लेता है और वह फिर जानबूझकर सतर्कतापूर्वक योजना बनाकर यह कार्य संपादित करने लग जाता है और इस प्रकार के कृत्यों की ओर तीव्रता से उन्मुख हो जाता है.

एक साधारण आदमी द्वारा भूख मिटाने हेतु की गई चोरी और बैंकिंग व्यवसाय में होनेवाली हेराफेरी दोनों अपराध एक जैसे होते हुए भी उन्हें अलग नजरिए से देखना अत्यंत आवश्यक है. एक आम आदमी और एक सफेदपोश आदमी द्वारा किए गए अपराध में इसलिए अंतर होता है, क्योंकि सफेदपोश आदमी जानबूझकर सतर्कतापूर्वक योजना बनाकर अपराधिक गतिविधि को अंजाम देता है, जिसका पता लगाना आसान नहीं होता.

बैंकिंग व्यवसाय में उदारीकरण, कम्प्यूटरीकरण, वैश्वीकरण, सूचना प्रौद्योगिकी तथा डिजिटल बैंकिंग के तहत अपराधों में काफी वृद्धि हुई है. सूचना प्रौद्योगिकी एवं डिजिटल बैंकिंग के विकास के मद्देनजर आधुनिक कम्प्यूटर, एटीएम, इंटरनेट बैंकिंग, टेली बैंकिंग, स्मार्ट कार्ड, डेबिट/क्रेडिट/ प्लास्टिक मनी कार्ड, मोबाइल बैंकिंग आदि का उपयोग अनिवार्य हो गया है. सूचना तकनीकी ने एक ओर विकास के नए आयाम खोल दिए तो दूसरी ओर विभिन्न अपराधिक गतिविधियों में बढ़ोत्तरी की. कहते है विकास के साथ–साथ विध्वंसक प्रवृत्तियां भी जन्म लेने लगती है, वास्तव में साइबर अपराध पर चर्चा करते है विस्तार से –

साइबर में ऐतिहासिक पार्श्वभूमि–

सन 1966 में अमरीकी रक्षा विभाग के एडवांस्ड रिसर्च प्रोजोक्टस ने सबसे पहले सूचनाओं को एक दूसरे तक पहंचाने के लिए इलेक्ट्रॉनिक विधियों को कंप्यूटरों के माध्यम से जोडकर नेटवर्क अपनिट तैयार किया था तथा 1969 में इसपर चार प्रोग्राम प्रोवाइडर कम्प्यूटरों को जोडा गया था. शुरू में इनका उपयोग रक्षा अनुसंधान से जुडे कार्यक्रम हेतु किया गया. 1989 में सर्व वैज्ञानिक टिम बर्नर्स ली ने वर्ल्ड वाइड वेब (डब्ल्यू डब्ल्यू डब्ल्यू) स्थापित किया. जो इंफार्मेशन ट्रेफिक (संग्रहण तथा संप्रेषण) का मूल आधार बना. इसके बाद तो आधुनिकता और गति का ऐसा समागम बना कि नित नई कार्य प्रणालियों ने दुनिया को आश्चर्यचकित कर दिया. ब्रॉडबैंड ऑप्टिकल फाइबर एवं उपग्रह प्रणाली ने सूचनाओं के आदान प्रदान में गति को तीव्र से तीव्रतम करके आधुनिक युग को सूचना क्रांति में परिवर्तित किया. जिसका सर्वाधिक प्रयोग बैंकिंग जगत में इंटरनेट बैंकिंग तथा मोबाइल बैंकिंग के रूप में हुआ.

सूचना प्रौद्योगिकी साइबर की देन –

सूचना प्रौद्योगिकी की खोज मानव इतिहास में पहिए की खोज के बाद दूसरी बड़ी खोज है, जिसने मानव के हर कार्यकलाप को प्रभावित किया है. पहिए के सहारे आप विश्व के किसी भी कोने में पहुंच सकते हो जबकि सूचना प्रौद्योगिकी के सहारे आपके सामने विश्व का कोई भी कोना प्रस्तुत हो सकता है. यही तो है बटन टेक्नोलॉजी का कमाल जो साइबर की देन है. वे दिन बहुत पीछे छूट गए जब हम अपने परिजनों को अपना संदेश भेजने के लिए कबूतरों की राह देखा करते थे. हमें पता भी ना चला कब इन डाकियों की जगह ई–मेल्स ने ले ली. आज का युग है बटन टेक्नॉलॉजी का अर्थात् क्लिक क्लिक क्लिक.

सूचना प्रौद्योगिकी का प्रभाव जीवन के सभी अंगों कारोबार, मुद्रा, सरकार, मीडीया, मनोरंजन आदी पर पडा है. ऐसे में भला वित्तीय क्षेत्र कंम्प्यूटल और इंटरनेट से अछूता कैसे रह सकता है? बैंकिंग जगत में प्रौद्योगिकी प्रवेश की प्रारंभिक अवस्था थी बैंकिंग में कम्प्यूटर का आना और धीरे धीरे आधुनिक बैंकिंग वन स्टॉप शॉप बन गयी.

साइबर अपराध परिभाषा –

कोई भी ऐसा कार्य जो कम्प्यूटर, इंटरनेट पर अवैधानिक तरीके से किया गया है एवं जिसमें बैंक संस्था अथवा ग्राहक की राशि का कपटपूर्ण आहरण, दुरूपयोग अथवा हानि शामिल को साइबर अपराध कहलाता है.

कम्प्यूटर से तात्पर्य सिर्फ कम्प्यूटर से न होकर मोबाइल फोन, लैपटॉप या फिर अन्य किसी यंत्र से है. जिसे इंटरनेट से जोड़ा जा सके. देखा जाए तो इसे 1820 में प्रथम साइबर अपराध रिकार्ड हुआ था जब गणक मशीन (केलक्यूलेटर) का उपयोग गलत मकसदों के लिए किया गया था.

शब्दजाल से बाहर निकलकर सरलतम शब्दों में कहें तो साइबर विकास के साथ जिन विध्वंसक प्रवृत्तियों का जन्म हुआ, उन्हें हम साइबर अपराध की श्रेणी में रखते है.

बैंकिंग जगत में साइबर अपराध–

आज आए दिन हम अखबारों में व समाचार में साइबर अपराधों के बारे में पढ़ते है, सुनते है व देखते है. जैसे जैसे हम बैंकिंग जगत में आधुनिक एवं उच्च प्रौद्योगिकी की तरफ बढ़ते हुए बैंकिंग को सुविधाजनक बनाते जा रहे है, वैसे वैसे साइबर अपराध के नए नए केस बढ़ते हुए नजर आ रहें है. 2013–14 में साइबर अपराध से संबंधित 10170 करोड़ की राशि के मामले सामने आए जब की मात्र एक वर्ष के अंदर आंकड़ा लगभग 100 प्रतिशत बढकर 19361 करोड़ हो गया. पिछले पांच वर्षों के आंकडे बताते है कि धोखाधडी के कुल मामलों का लगभग 65 प्रतिशत प्रौद्योगिकी विशेषकर इंटरनेट बैंकिंग, एटीएम, क्रेडिट / प्रीपेड कार्ड आदि से संबंधित रहा. साइबर अपराधों का सुरक्षा की मुख की तरफ बढ़ना स्वाभाविक भी है क्योंकि नोटबंदी और डिजिटल बैंकिंग में हुई अभूतपूर्व वृद्धि के कारण पैसा अब न केवल मूर्त रूप में बल्कि ज्यादातर इलेक्ट्रॉनिक माध्यम से इधर से उधर हो रहा है. इससे गलत तत्वों को शह मिलती है कि वे इसे सूचना के माध्यम से ही चुराने के लिए गलत तरीकों का इस्तेमाल करें.

आक्रमणकारियों का सबसे अधिक लक्ष्य ग्राहक के विवरण जानने का होता है क्योंकि इससे उन्हें खजाने की चाबी प्राप्त हो जाती है. अब बढ़ते है साइबर अपराध के वर्गीकरण की ओर –

साइबर अपराध का वर्गीकरण–

साइबर अपराध को हम दो वर्गों में बांट सकते है जैसे–

किंग, वायरस वर्ग तथा डेटा आपरेटिंग सिस्टम (डॉस) में कम्प्यूटर को एक लक्ष्य के रूप में रखकर अन्य कम्प्यूटर पर आक्रमण करना.

कम्प्यूटर का उपयोग हथियार के रूप में करके किसी का खाता या क्रेडिट कार्ड लेकर वित्तीय धोखाधड़ी करना या किसी के डेटा व सूचनाओं से छेड़छाड़ करके अपराध को कार्यान्वित करना.

बैंकिंग से संबंधित साइबर अपराध निम्न है–

1. कार्ड की चोरी – क्रेडिट कार्ड को चुराकर अधिकांश अपराध किए जाते है, जिनमे परिवार के सदस्य तथा मित्र भी शामिल है.
2. सूचनाओं की चोरी– स्किमिंग) –कभी कभी दुकानदारों के नौकर चाकर हैकरों की गिरोह से मिलीभगत कर कार्ड का डेटा चुरा लेते है और डुपलिकेट कार्ड बनाकर अपराध को अंजाम देते है.
3. व्यक्तिगत सूचनाओं से धोखाधड़ी – अपराधी ग्राहक से संबंधित व्यक्तिगत सूचनाएं जैसे जन्मतिथि, पता प्राप्त कर बैंक से पता बदलने का अनुरोध करते है. फिर कार्ड खोने की तकार करते हुए नया कार्ड प्राप्त कर अपराध करते है.
4. ग्राहक के नाम से कार्ड प्राप्त करना – केवाईसी के लिए नकली दस्तावेज प्रस्तुत करके पूरी प्लानिंग से नया खाता खोलकर बैंक से क्रेडिट कार्ड लिया जाता है और अपराध को अंजाम दिया जाता है.
5. एटीएम का प्रयोग – एटीएम का प्रयोग करते हुए लेन–देन को अधूरा छोड़ देने की स्थिति में अधिकतर अपराध होते है.
6. नेट बैंकिंग – इसके अंतर्गत फर्जी वेबसाइट खुलने से ग्राहक अपना पिन नंबर और डिटेल फीड करता है जिसके जरिए अपराध करने में आसानी होती है.
7. डेटा डिडलिंग तथा इंटरनेट टाइम चोरी – प्रोसेसिंग होने से पूर्व कम्प्यूटर पर डेटा बदल देना तथा प्रोसेस के बाद उसे पूर्व रूप में बदल देना डेटा डिडलिंग होता है.
8. इंटरनेट पायरेसी – इसका अर्थ है किसी कॉपीराइट फाइल का इंटरनेट के माध्यम से गैरकानूनी तरीके से चुराना.

चलिए अब एक नजर डालते है साइबर अपराध के विभिन्न प्रकारों पर –

साइबर अपराध के विभिन्न प्रकार – इनमें निम्न शामिल है–

1. फिशिंग – यह भ्रामक मैलबेयर एवं डीएनएस आधारित आपराधिक प्रक्रिया है, जिसके द्वारा नकली पहचान बनाकर संवेदनशील जानकारी जैसे उपयोगकर्ता का नाम, पासवर्ड, क्रेडिट कार्ड का विवरण, आदि की चोरी की जाती है.
2. स्निफर – यह मूलतः रिकार्डिंग सॉफ्टवेयर है जिसका विकास नेटवर्क के रखरखाव हेतु किया गया था. इसका प्रयोग करके नेटवर्क पर भेजी जा रही सूचनाएं चोरी कर ली जाती है.
3. पासवर्ड की चोरी– यह मुख्यतः अनुमान के द्वारा या डिफॉल्ट पासवर्ड द्वारा की जाती है. इनमें शब्दकोश आधारित हमले एवं ब्रूट फोर्स हमले भी शामिल है.

4. आइपी स्पूफिंग या पहचान हमला – इसमें हमलावर अपने स्त्रोत कम्प्यूटर की पहचान छुपाकर, नकली पहचान धारण करके अपराध करता है.
5. इनपुट मान्यकरण हमला – इनपुट सत्यापन हमले खराब प्रोग्रामिंग की वजह से तब होते है, जब इनपुट स्वीकार करने से पहले इसे मान्य करने के लिए की जानेवाली प्रक्रिया ठीक तरह से काम न कर रही हो.
6. एक्सयूएल इंजेक्सन हमला – यह एप्लीकेशन की कमजोरी की वजह से होता है जहां डेटाबेस क्वेरी इंटरनेट के माध्यम से की जाती है और वेबपेज में सत्यापन नहीं होता.
7. सेवा रोकनेवाले हमले – यह वेबसाइट पर सामान्य गतिविधि को रोकने के इरादे से किए जाते है, जैसे स्नर्फ, सिन.
8. मध्य में आदमी हमला – इसमें डेटा भेजने के बाद रास्ते में उसकी नकल करके चोरी की जाती है.
9. सोशल इंजीनियरिंग हमला – सिस्टम व्यवस्थापक होने का दिखावा करके संवेदनशील जानकारी जैसे पासवर्ड, एकांउट नंबर , पते तथा क्रेडिट कार्ड नंबर हासिल करते है.
10. क्रॉस साइट रिक्वेस्ट फोर्जरी हमला – यह जाली लेन–देन के अनुरोध पर किया जाता है.
11. ई – मेल फोजिंग – ई मेल इस तरह से भेजा जाता है मानो यह किसी अधिकारिक स्थान से भेजा हो और इसके जरिए सारी सूचनाएं प्राप्त की जाती है. जिसका कालांतर में दुरूपयोग किया जाता है.

चलिए अब चर्चा को आगे बढ़ाते हुए जानते है बैंकिंग में साइबर अपराध के कारण –

बैंकिंग क्षेत्र में बढ़ते हुए साइबर अपराध के कारण –

सूचना क्रांति के बाद वैश्विक अर्थव्यवस्था के साथ साथ बैंकिंग जगत में नए युग की शुरूआत हुई. सूचना प्रौद्योगिकी के अनुप्रयोग से बैंकिंग विश्व एक ब्रह्मांड. सार्वभौम केन्द्र के अन्तर्गत समाहित हो गया और समस्त विश्व एक माउस की क्लिक पर आकर ठहर गया जिसे हम बटन दबाते सेवा का यूग कहते है. जिसके मद्देनजर बैंकिंग उद्योग में कपट, जालसाजी, धोखाधडी, गबन जैसी आपराधिक गतिविधियों में काफी वृद्धि हुई है. विशेषकर साइबर अपराध एक गंभीर चुनौती के रूप में उभर रहें है. चिंता की बात यह है कि दिन–ब–दिन साइबर अपराध के मामले अत्यंत क्लिष्ट और उलझे हुए नजर आ रहे है.

बैंकिंग क्षेत्र में सुरक्षा की मुख की तरफ बढ़ते साइबर अपराधों के निम्न मुख्य कारण है –

1. लालच – श्रीमद् भगवत गीता में भगवान – श्रीकृष्ण ने लालच को नरक का द्वार संबोधित कर यह सिद्ध किया है कि अपराध का मुख्य कारण लालच या ग्रीड है न कि जरूरत अथवा नीड. सफेदपोश साइबर अपराधों का मुख्य हेतु बगैर कुछ किए , कुछ पाने का लालच है. जाहिर है तकनीक का विकास इस्तेमाल और दुरूपयोग इंसान के द्वारा ही होता है.
2. अशिक्षा – शिक्षा के अभाव के कारण गोपनीय सूचनाओं जैसै जन्मदिनांक, पिन नंबर आदि बताकर ग्राहक अपराधी का शिकार होते है.
3. असावधानी – एटीएम से पैसे निकालने के बाद ग्राहक कार्ड या पर्ची वहीं छोड़ते है, जिसका अपराधी दुरूपयोग करता है.
4. सुनियोजित ढंग से साइबर अपराधों का कार्यान्वयन – स्वंय को बैंक का अधिकारी दर्शाते हुए ग्राहक के द्वारा सूचना न देने पर खाता या कार्ड को ब्लॉक हो जाने की बात कर भोलेभाले ग्राहकों को अपने जाल में फंसाया जाता है. अपराधी फोन पर कुछ इस अंदाज में बात करते है कि अल्पशिक्षित और अशिक्षित तो क्यों शिक्षित लोग भी उनके झांसे में आ जाते है. वे बडे ही नियोजित तरीके से भ्रमित कर ठगते है, जिसका स्पस्ट उदाहरण उनके द्वारा पीड़ित हो चुके प्रशासनिक अधिकारी, पुलिस अधिकारी, न्यायिक अधिकारी तथा स्वयं बैंक अधिकारी भी है.

साइबर अपराधों की ताजा घटनाएं – जो न केवल बैंकों के लिए बेहद चुनौतीपूर्ण है, बल्कि ग्राहकों के लिए भी चिंता का विषय है, जिनमें निम्न शामिल है –

1. 2 अगस्त 2016 को बिटफिनेक्स डिजिटल करेंसी की ट्रेडिंग के लिए हांगकांग एक्सचेंज ने घोषणा की कि उसके कुछ ग्राहकों के खाते हैक कर लिए गए है और बिटक्वाइन चोरी कर लिए गए है, जिनका मूल्य तकरीबन 65 मिलियन अमरीकी डालर था. फलस्वरूप बिटक्वाइन का मूल्य गिर गया और डिजिटल करेंसी से लोगों का भरोसा हिल गया.
2. भारत में एक कामर्शियल बैंक के नास्ट्रो खाते में धोखे से भुगतान अनुदेश जारी किए गए और उसे स्विफ्ट संदेश प्रणाली पर रखा जा रहा था. यद्यपि संबंधित भुगतान कर्ता मध्यस्थता करने वाले बैंक के साथ अनुवर्तन किए जाने से मौद्रिक नुकसान से बचें.
3. बांग्लादेश बैंक को निशाना बनाकर बिलियन अमरीकी डालर चोरी करने का प्रयास किया गया और अंततः आक्रमणकारी 81 बिलियन डालर लेकर भाग गए.

4. एक बडे बैंक के ई पेमेंट वेबसाईट को हैक कर लिया गया. आश्चर्य की बात तो यह है कि उस बैंक ने उसे तब तक नोटिस नहीं किया जब तक की एक विधि प्रवर्तन एजेंसी ने नोटिस करके नहीं बताया.

5. एक बैंक के मोबाईल वैलैट को साझा किया गया, जिसमें संवदेनशीलता एप्लीकेशन में ही पाई गई, जिसका दुरूपयोग आक्रमणकारी द्वारा किया गया.

6. साइबर अपराधों की घटनाएं अधिकांशतः अंतिम उपभोक्ता को निशाना बनाने के बजाए वित्तीय संस्थाओं को लक्ष्य करने की ओर बढ़ती जा रही है, जिसका जीता– जागता उदाहरण कार बनाक गिरोह है, कारबनाक गिरोह ने उपभोक्ता के ब्यौरे चुराने के साइबर अपराधी तरीके अपनाने के बजाए बैंक की आंतरिक प्रणाली और परिचालनों को लक्ष्य करके अनेक चैनलों में डकैती डालकर लगभग 1 बिलियन अमरीकी डालर की चोरी की.

हालांकि, बैंकिंग व्यवसाय का आधार ही आपसी विश्वास है किंतु साइबर सुरक्षा के मामले में जीरो–ट्रस्ट पॉलिसी अपनाना बेहद आवश्यक है. इन घटनाओं को देखते हुए, आज साइबर सुरक्षा समय की मांग है. देखते है विस्तार से –

साइबर अपराधों की रोकथाम हेतु सुरक्षात्मक उपाय – (वैश्विक)

पूरे विश्व में अब फोकस साइबर सुरक्षा पर है. साइबर सुरक्षा अब किसी भी तरह से प्रथक घटना नहीं है जो केवल एक उद्योग या देश को प्रभावित कर रही है. अनेक साइबर आक्रमणकारी जिनमें संगठित गिरोह तथा राष्ट्र – राज्य के एक्टर्स भी शामिल होते है. यह आक्रमण राजनैतिक, धार्मिक उद्देश्य की पूर्ति तथा आतंकवाद को बढ़ावा देने के लिए किए जाते है. इस मुद्दे के महत्व का अंदाजा इस बात से लगाया जा सकता है कि विश्व की मानक निर्धारक निकाय तथा प्रतिष्ठित केन्द्रीय बैंक इस तबाही को दूर करने के लिए बहुत बड़े संसाधनों को लगा रहे हैं.

सूचना सुरक्षा का अर्थ है – सूचना को सुरक्षित रखना एवं सूचना प्रणालियों का अनाधिकृत पहुंच से बचाना तथा उनके दुरूपयोग, प्रकटीकरण, विघटन , संशोधन, अवलोकन, निरीक्षण, रिकार्डिंग अथवा उनको नष्ट होने से सुरक्षित रखना.

एलेन ग्रीन स्पेन के शब्दों में धोखाधड़ी, गबन, भ्रष्टाचार हर जगह मौजूद है, खेद है कि मानव जाति की यह स्वाभावतः कमजोरी है, किसी भी सफल अर्थव्यवस्था को बस इतना जरूर करना चाहिए कि वह इन्हें कम से कम रखें.

बिल गेट्स का कहना है कारोबार में उपयोग की जानेवाली किसी प्रौद्योगिकी का पहला नियम है की किसी कुशल परिचालन में स्वचालकता लागू कर दी जाए तो उसकी कुशलता में काफी इजाफा होता है. दूसरा नियम है कि किसी अकुशल परिचालन में स्वचालकता लागू कर दी जाए तो उसकी अकुशलता में काफी इजाफा होता है.

उदारीकरण, निजीकरण, वैश्वीकरण तथा सूचना प्रौद्योगिकी और डिजिटलीकरण के दौर में बैंकिंग जगत में साइबर अपराध एक गंभीर चुनौती के रूप में उभर रहे है. जालसाजों के लिए पैसे उडाना उनके बायें हाथ का खेल बन गया है. जितना ज्यादा ऑनलाइन बैंकिंग हम करते है, उतना ही ज्यादा ये जालसाज फिशिंग और पासवर्ड हाइजैकिंग करते है. आइए साइबर अपराध के रोकथाम पर चर्चा करते है भारतीय परिप्रेक्ष्य में –

भारत सरकार ने साइबर आक्रमण के खतरे को दूर करने के लिए अनेक कदम उठाए है और महत्वपूर्ण संस्थागत व्यवस्थाएं की है. भारतीय कम्प्यूटर एमरजेंस रिस्पांस टीम (सीईआरटीई) की स्थापना की गई है जो भारतीय साइबर स्पेस की निगरानी करती है और बड़े खतरों के प्रति सजग एवं सतर्क करने में समन्वयक का कार्य करती है. राष्ट्रीय साइबर समन्वयन केन्द्र की स्थापना भी इसी उपलक्ष्य में की गई.

भारतीय रिज़र्व बैंक ने 2 जून 2016 को बैंकों में साइबर सुरक्षा संरचना के संबंध में अनुदेश जारी किए है. इसके तहत बैंक अपने बोर्ड द्वारा अनुमोदित साइबर सुरक्षा संरचना नीति लागू करें ताकि साइबर – संकट प्रबंधन योजना बनाई जा सकें, निरंतर चौकसी की व्यवस्था की जा सके, हार्डवेयर, साफ्टवेयर, नेटवर्क डिवाइसेस आदि खरीदते समय. कनेक्ट करते समय सुरक्षा परलुओं का आकलन किया जा सके, उपभोक्ता सूचना की रक्षा सुनिश्चित की जा सके, तथा साइबर सुरक्षा की तैयारी में कमी का मूल्यांकन किया जा सकें.

बैंकिंग में साइबर अपराध की रोकथाम हेतु दंडात्मक उपाय –

आईटी एक्ट 2000 हमें ई कॉमर्स तथा डिजिटल हस्ताक्षर की विस्तृत जानकारी देता है. साइबर अपराध एक दंडनीय अपराध है और इसकी रिपोर्टिंग तुरंत ही की जानी चाहिए. स्थानीय पुलिस स्टेशन या मुख्य नियंत्रण कक्ष (नं. 100) को पीडित व्यक्ति या अपराध की जानकारी रखने वाला अन्य व्यक्ति भी ऑनलाइन रिपोर्टिंग कर सकता है.

साइबर क्राइम थानों का आधुनिकिकरण – समय की मांग –

बढ़ते हुए साइबर अपराधों को देखते हुए साइबर अपराधियों को पकड़ने के लिए पुलिस यंत्रणा तथा साइबर क्राइम थानों के आधुनिकीकरण की आवश्यकता है. पुलिस विभाग के कर्मियों को आधुनिक तकनीक और प्रौद्योगिकी की जानकारी एवं

विशेष ट्रेनिंग उपलब्ध कराना समय की मांग है. तभी वे कुशलतापूर्वक साइबर अपराधियों से निपट सकेगें. जहां तकनीक अपग्रेड हुई है तो पुलिस को भी अपडेट होना होगा. अब चर्चा को बढ़ाते है निवारक सतर्कता की ओर –

बैंकिंग में साइबर अपराध की रोकथाम हेतु निवारणात्मक उपाय –

अंग्रेजी में एक प्रसिद्ध कहावत है प्रिवेंशन इज बेटर देन क्यूअर अर्थात् परहेज इलाज से बेहतर है. निवारक सतर्कता वह अवधारणा है जिसके तहत अपराधिक गतिविधियों को घटने / रोकने के सुरक्षात्मक एवं निवाराणात्मक उपायों से हम रूबरू होते है जैसे –

1. ग्राहक को जागरूक बनाने की आवश्यकता – ग्राहकों को साइबर अपराध से बचाव हेतु जागरूक बनाने के लिए बैंकों में पैम्फलेट का वितरण शाखाओं में वीडियो के माध्यम से जानकारी, डाक्यूमेन्ट्री का प्रदर्शन , टेलीविजन , पत्र – पत्रिकाओं के माध्यम से विज्ञापन देना जरूरी है, ताकि वे ठगे जाने से बचें.
2. ग्राहक के द्वारा सावधानी बरतना – आइडी और पासवर्ड जैसी गोपनीय सूचना को गुप्त रखना, इंटरनेट बैंकिंग सिर्फ अपनी पीसी से करना ना कि साइबर कैफे से तथा इंटरनेट बैंकिंग इस्तेमाल करने के बाद उसे लॉगआउट करना, मोबाइल नंबर को खाते में अपडेट करना ताकि खाते के लेन – देन की जानकारी प्राप्त हो सके. जैसी बातों पर ग्राहक के द्वारा सावधानी बरतना.
3. एटीएम में प्रभावी कैमरा – इससे अपराधी के द्वारा रकम आहरण की स्थिति में उसकी पहचान सुनिश्चित होगी.
4. मोबाइल फोन से सूचना – जिस प्रकार अपराधी मोबाइल पर जनता को गुमराह करनेवाली सूचना देते है उसी प्रकार ग्राहकों को इन धोखाधड़ी वाले प्रस्ताव से बचने के लिए संदेश दिया जा सकता है. लगातार संदेश प्राप्त होने पर ग्राहकों में जागरूकता आएगी.
5. स्थानीय भाषा में जानकारी – ग्राहकों को स्थानीय अथवा समझने योग्य भाषा में जानकारी दी जानी चाहिए, ताकि वे लॉटरी नौकरी या अन्य प्रलोभन के चक्कर में पड़ने से बचें.
6. एडवांस्ड सिक्योरिटी सिस्टम तथा मान्यता प्राप्त सॉफ्टवेयर का उपयोग – सभी कम्प्यूटरों में लोड करना आवश्यक है. बैंकर को किसी अनजान व्यक्ति की पेन ड्राइव या सीडी अपने सिस्टम पर नहीं लगानी चाहिए ताकि वायरस से बचाव किया जा सके. बैंकिंग जगत में बढ़ते हुए साइबर अपराध को रोकथाम हेतु निवारक सतर्कता एक कारगर उपाय है.

उपसंहार –

सूचना प्रौद्योगिकी और डिजिटलीकरण के दौर में साइबर अपराधों ने बैंकिंग जगत को अपने चपेट में ले लिया है. बैंकों को देश के आर्थिक विकास का बैरोमीटर समझा जाता है. वह वास्तविक सेक्टरों से सम्बद्धता के कारण डिपोजिटरी संस्थान के रूप में सार्वजनिक रकम के संरक्षक या कस्टोडियन है. बैंकिंग व्यवस्था सामाजिक रूपांतरण का ऐसा प्रभावी माध्यम है जो त्वरित आर्थिक विकास के साथ साथ सामाजिक लक्ष्यों की प्राप्ती हेतु समुचित वातावरण के निर्माण में सहायक सिद्ध हुई है. अतः बैंकों के लिए यह आवश्यक है कि वे अपने सामाजिक, आर्थिक दायित्वों का निर्वाहन करने के साथ ही जमा राशियों की सुरक्षा का उत्तरदायित्व भी भलीभांति निभाएं. यदि बैंकों को अपनी नींव सुदृढ़ रखनी है, ग्राहकों का विश्वास बरकरार रखना है, अर्थव्यवस्था को चलाने में अपनी अहम भूमिका सुचारू रूप से निभानी है तो आवश्यक है कि वे अपना कॉरपोरेट गवर्नेन्स सुधारें, दुर्भेद्य आईटी सिस्टम लगाएं, प्रभावी नीतियां और कार्यविधियां बनाएं, मानदंडो का कडाई से अनुपालन करें अपितु साइबर अपराधियों के खिलाफ कठोर कार्रवाई करने में कोताही न बरतें.

बैंक व्यवसाय की सफलता अपने ग्राहकों के प्रदान की जानेवाली सेवाओं की प्रभावकारिता, दक्षता और सुरक्षितता पर निर्भर करती है. बैंकों के प्रति ग्राहकों का विश्वास बदस्तूर रहें उनके लेन – देन सुरक्षित रहें, उनमें गोपनीयता रहें, ग्राहकों की सूचनाओं का सत्यापन हो सके, इसके लिए बैंकों को केवल कार्यालय या शाखा स्तर पर ही नहीं बल्कि प्रत्येक कर्मचारी स्तर पर सजग और सतर्क रहना होगा. एक संतुष्ट एवं प्रसन्न ग्राहक, समूह उन्नति व लाभप्रदता के लिए सर्वोत्तम अदत्त प्रचार अभिकर्ता है, जोकि नए ग्राहक सृजित करने के उपाय निकालता है, जिसका आशय है और अधिक व्यवसाय.

बैंकों को एक ओर साइबर अपराधों से त्रस्त ग्राहकों की पसीने की कमाई को एवं ग्राहकों के नजर में अपनी छवि को धूमिल होने से बचाते हुए ग्राहकों के हितों की रक्षा करनी है तो दूसरी ओर सुरक्षा की मुख की तरफ बढ़ते हुए साइबर अपराधों की रोकथाम हेतु हर संभव कोशिश करते हुए डिजिटल बैंकिंग की लोकप्रियता को सजगता और सतर्कतापूर्वक बरकरार रखनी है.

मीरा कोठावले
सहायक प्रबंधक
सेन्ट्रल बैंक ऑफ इंडिया

पुस्तकें वे साधन हैं जिसकी मदद से हम
संस्कृतियों के बीच पुल बनाते हैं (यानी, संस्कृतियों को जोड़ते हैं).

–डॉ. सर्वपल्ली राधाकृष्णन

किताब के अंदर एकमात्र महत्व की चीज है
आपके लिए उसमें निहित अर्थ.

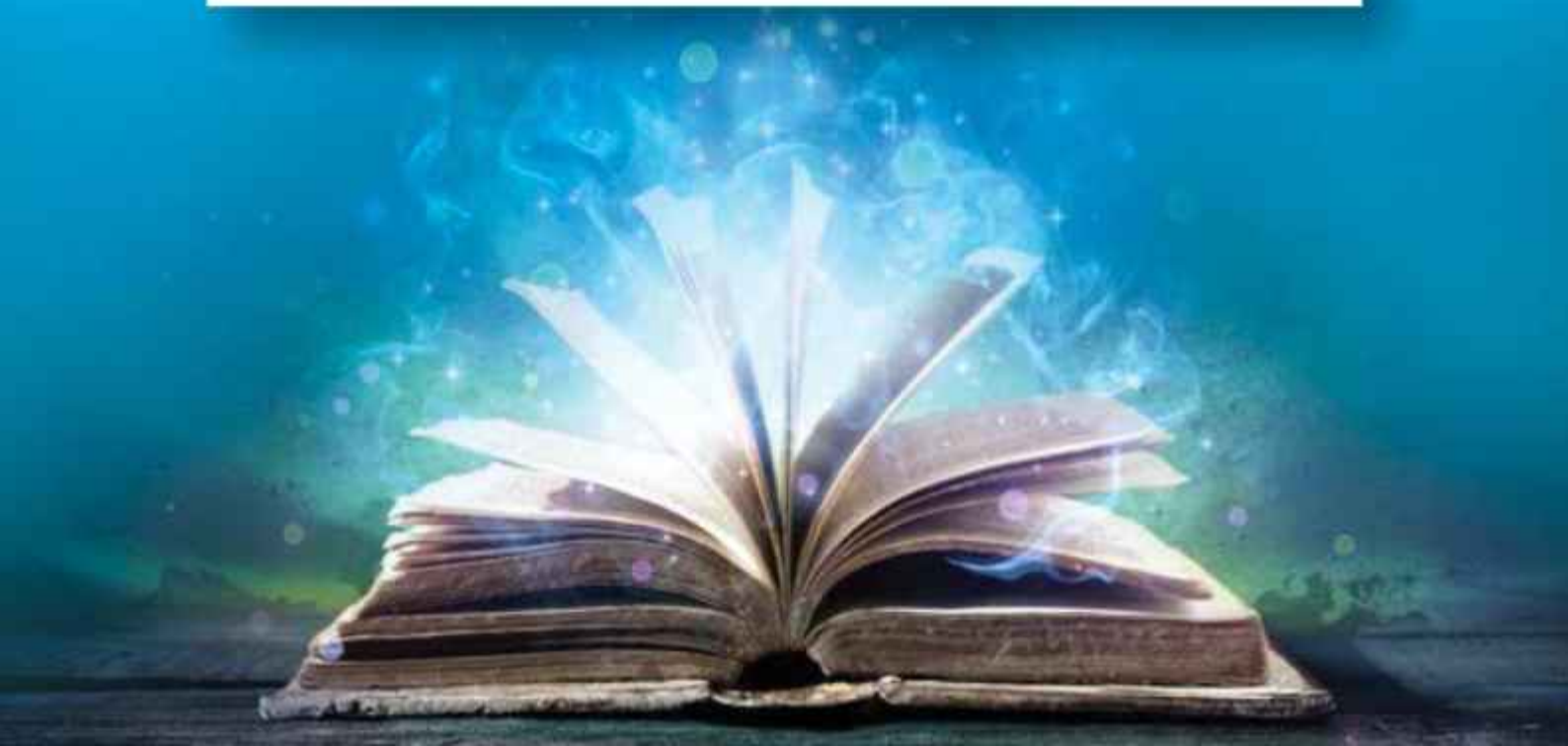
–डब्ल्यू. सॉमरसेट

एक बार जब आप पढ़ना सीख लेते हैं,
तो हमेशा के लिए आजाद हो जाते हैं.

–फ्रेडरिक डगलस

एक चीज जो आपको बिल्कुल सही–सही जाननी चाहिए
वह है लाइब्रेरी का पता.

–अल्बर्ट आइंसटाइन



सेन्ट्रल बैंक ऑफ़ इंडिया
Central Bank of India
1911 से आपके लिए "सेंट्रल" "CENTRAL" TO YOU SINCE 1911

सत्यमेव जयते

हमारा संविधान एक जीवंत दस्तावेज़ है, जो स्वतंत्रता, न्याय और समानता के प्रति हमारी प्रतिबद्धता की निरंतर याद दिलाता है।

आइए हम इसके सिद्धांतों की रक्षा करें और उन्हें बनाए रखें

www.centralbankindia.co.in