सशक्त सहकारिता ; समृद्ध मध्य प्रदेश

अपेक्स बैंक

# साइबर सुरक्षा

# (आवश्यक दिशानिर्देश)


## म.प्र. राज्य सहकारी बैंक (अपेक्स बैंक)

**न्यू मार्केट, टी.टी. नगर, भोपाल 462003**

# अनुक्रमणिका

# साइबर सिक्युरिटी: संक्षिप्त परिचय

## 1.1 साइबर सिक्युरिटी क्या है?

साइबर सिक्युरिटी डिजिटल हमलों से सिस्टम, नेटवर्क और प्रोग्राम की रक्षा करने का अभ्यास है। ये हमले आमतौर पर संवेदनशील जानकारी तक पहुँचने, बदलने या नष्ट करने के उद्देश्य से होते हैं; इसके जरिये अपराधी या तो यूजर्स से पैसा निकालना या सामान्य व्यावसायिक प्रक्रियाओं को बाधित करना चाहते हैं।

प्रभावी साइबर सिक्युरिटी उपायों को लागू करना आज विशेष रूप से चुनौतीपूर्ण है क्योंकि लोगों की तुलना में अधिक डिवाइसेस हैं, और हमलावर अधिक अभिनव बन रहे हैं। साइबर सुरक्षा में कई बार खतरा इसलिए है क्योंकि नेटवर्क कनेक्शन और इंटरनेट काफी तेज़ी से दुनिया को बदलता जा रहा है। इस वजह से सुरक्षा काफी महत्वपूर्ण हो गयी है।

साइबर सुरक्षा और सुरक्षा फोर्स दोनों ही डाटा की सुरक्षा के लिए रखे जाते हैं जिससे कि किसी भी तरह से डाटा की चोरी न हो और सभी डॉकयुमेंट और फाइल सुरक्षित रहें।

## 1.2 साइबर सिक्युरिटी क्यों महत्वपूर्ण है (Importance of Cyber Security):

कौन सी बात साइबर सिक्युरिटी को इतना महत्वपूर्ण बनाती है? अधिकांश कंपनियां आज कंप्यूटर डेटाबेस पर अधिक से अधिक इनफॉर्मेशन स्टोर कर रही हैं। जब आप व्यक्तिगत रूप से इंटरनेट से कनेक्ट होते हैं या अपने क्रेडिट के साथ खरीदारी करते हैं, तो न केवल आपकी जानकारी जोखिम में होती है, बल्कि दिन के लगभग किसी भी समय इसमें सेंध लगने का जोखिम भी होता है।

सरकार, सैन्य, वित्तीय संस्थान, विभिन्न निगम, अस्पताल और कई अन्य व्यवसाय प्रक्रियाएं करते हैं और अपने नेटवर्क पर आपकी इनफॉर्मेशन स्टोर करते हैं। जबकि इन आर्गेनाइजेशन्स द्वारा परिष्कृत सिक्युरिटी रणनीति का उपयोग किया जाता है, लेकिन इस बात की गारंटी देने का कोई तरीका नहीं है कि आपकी जानकारी हमेशा सुरक्षित हो।

आने वाले वर्षों में, नई तकनीकों और इरादों का उपयोग करके और भी अधिक एडवांस साइबर हमले होंगे। डार्क वेब (**Dark Web**) पर रैनसमवेयर और मालवेयर की उपलब्धता में नाटकीय वृद्धि होगी।

## 1.3 साइबर सिक्युरिटी के तीन स्तंभ

**1) People: प्रत्येक कर्मचारी को साइबर खतरों को रोकने और कम करने में उनकी भूमिका के बारे में पता होना चाहिए, और विशेष तकनीकी साइबर सिक्युरिटी कर्मचारियों को साइबर हमलों को कम करने और प्रतिक्रिया देने के लिए नवीनतम कौशल और योग्यता के साथ पूरी तरह से तैयार रहने की आवश्यकता है।**

**2) Processes: आर्गेनाइजेशन की जानकारी के जोखिमों को कम करने के लिए आर्गेनाइजेशन की गतिविधियों, भूमिकाओं और प्रलेखन का उपयोग कैसे किया जाता है, इसे परिभाषित करने में प्रक्रियाएं महत्वपूर्ण हैं। साइबर खतरे जल्दी से बदलते हैं, इसलिए प्रक्रियाओं को उनके साथ अनुकूलन करने में सक्षम होने के लिए लगातार समीक्षा करने की आवश्यकता होती है।**

**3) Technology: उन साइबर जोखिमों की पहचान करके, जो आपके आर्गेनाइजेशन का सामना करते हैं, तब आप यह देखना शुरू कर सकते हैं कि किस स्थान पर नियंत्रण करना है, और इसके लिए आपको किन तकनीकों की आवश्यकता होगी। साइबर जोखिमों के प्रभाव को रोकने या कम करने के लिए प्रौद्योगिकी को तैनात किया जा सकता है, जो आपके जोखिम मूल्यांकन और आपके जोखिम के स्वीकार्य स्तर पर निर्भर करते हैं।**

### साइबर सिक्युरिटी के प्रकार (Types of Cybersecurity)

**यह शब्द विभिन्न प्रकार के संदर्भों में लागू होता है, व्यवसाय से मोबाइल कंप्यूटिंग तक, और कुछ सामान्य श्रेणियों में विभाजित किया जा सकता है।**

1. **Network Security: नेटवर्क सिक्युरिटी घुसपैठियों से कंप्यूटर नेटवर्क को सुरक्षित करने का अभ्यास है, चाहे लक्षित हमलावर या अवसरवादी मैलवेयर।**
2. **Application Security:**
   **एप्लिकेशन सिक्युरिटी, सॉफ़्टवेयर और डिवाइसेस को खतरों से मुक्त रखने पर केंद्रित है। एक समझौता किए गए एप्लिकेशन, सिक्युरिटी के लिए डिज़ाइन किए गए डेटा का एक्सेस प्रदान कर सकता है। डिजाइन स्टेप में सफल सिक्युरिटी शुरू होती है, इससे पहले कि कोई प्रोग्राम या डिवाइस तैनात किया जाता है।**
3. **Information Security:**
   **इनफॉर्मेशन सिक्युरिटी, डेटा की अखंडता और प्राइवेसी की रक्षा करती है, दोनों स्टोरेज और ट्रांजिट में।**

4. **Operational Security: ऑपरेशनल सिक्युरिटी में डेटा एसेट को संभालने और उनकी सिक्युरिटी के लिए प्रक्रियाएं और निर्णय शामिल हैं। किसी नेटवर्क तक पहुँचने के दौरान यूजर की अनुमतियाँ और यह निर्धारित करने की प्रक्रियाएँ कि डेटा को कैसे और कहाँ स्टोर या शेयर किया जा सकता है सभी इस सिक्युरिटी के नीचे आते हैं।**
5. **Disaster Recovery and Business Continuity: यह सिक्युरिटी यह परिभाषित करती है कि कैसे एक ऑर्गनाइज़ेशन साइबर सिक्युरिटी घटना या किसी अन्य घटना पर प्रतिक्रिया करता है जो संचालन या डेटा के नुकसान का कारण बनता है। डिजास्टर रिकवरी की पॉलिसी यह बताती हैं कि ऑर्गनाइज़ेशन अपने परिचालन और सूचनाओं को उसी परिचालन क्षमता पर वापस लाता है जैसे कि हमले से पहले था। व्यवसाय की निरंतरता वह योजना है जिसे ऑर्गनाइज़ेशन कुछ संसाधनों के बिना संचालित करने की कोशिश में वापस आता है।**
6. **End-User Education: एंड-यूजर एजूकेशन सबसे अप्रत्याशित साइबर-सिक्युरिटी फैक्टर को संबोधित करती है: लोग। कोई भी गलती से अच्छी सिक्युरिटी प्रथाओं का पालन करने में विफल रहने से एक वायरस को सिक्युरिटी सिस्टम में ला सकता है। किसी भी ऑर्गनाइज़ेशन की सिक्युरिटी के लिए यूजर्स को संदेहास्पद ईमेल अटैचमेंट को हटाना, अज्ञात USB ड्राइव को प्लग इन न करना, और विभिन्न अन्य महत्वपूर्ण सबक सीखने चाहिए।**

# बैंकिंग में साइबर सुरक्षा

## 2.1 बैंकिंग में साइबर सुरक्षा का महत्व

सूचना और प्राद्योगिकी (Information & Technology) में हो रहे तेज बदलाओं के फलस्वरूप बैंकिंग प्रणाली परिदृश्य में भी बदलाव आ रहे हैं।अब बैंकिंग सुविधाएँ 24*7 घण्टे उपलब्ध हैं आप अपने मोबाइल, लैपटॉप, डेस्कटॉप आदि से पैसे का लेन देन कहीं भी किसी भी वक़्त कर सकते हैं. यह सब नयी तकनीकें ग्राहक और बैंकर्स के बीच के परस्पर संबंधों को भी नयी दिशा और दशा प्रदान कर रही हैं। इन सबके फलस्वरूप वित्तीय क्षेत्र में साइबर सुरक्षा का बहुत महत्व रहा है। बैंकिंग विश्वास और भरोसे का दूसरा नाम आज की बैंकिंग कैशलेस (नकदी का कम उपयोग) की तरफ अग्रसर है, उदाहरणतः डेबिट कार्ड, क्रेडिट कार्ड और इंटरनेट बैंकिंग आदि का उपयोग दिनों दिन बढ़ रहा है। इस संदर्भ में, यह सुनिश्चित करना बहुत महत्वपूर्ण हो जाता है कि बैंक डेटा और उसकी गोपनीयता की सुरक्षा के लिए साइबर सुरक्षा के सभी उपाय किये जाएँ।

जैसे-जैसे व्यक्ति और कंपनियां ऑनलाइन अधिकांश लेन-देन करती हैं, डेटा भंग होने का जोखिम रोज बढ़ता है। यही कारण है कि बैंकिंग क्षेत्र की प्रक्रियाओं में साइबर सुरक्षा पर अधिक जोर दिया गया है। आज अधिक व्यक्ति मोबाइल एप्लिकेशन पर अपने बैंक खाते तक पहुंचते हैं। इनमें से कई लोगों के पास कम से कम या कोई सुरक्षा नहीं है, और इससे हमले की संभावना बहुत अधिक हो जाती है। इसलिए, दुर्भावनापूर्ण गतिविधि को रोकने के लिए समापन बिंदु पर बैंकिंग सॉफ़्टवेयर में सुरक्षा हेतु प्रावधान आवश्यक हैं।

बैंकिंग क्षेत्र के लेनदेन में साइबर सुरक्षा के महत्व का स्पष्ट कारण ग्राहक परिसंपत्तियों की रक्षा करना है। जैसे-जैसे अधिक लोग कैशलेस होते जाते हैं, गतिविधियाँ ऑनलाइन चेकआउट पृष्ठों और भौतिक क्रेडिट स्कैनर के माध्यम से की जाती हैं। दोनों स्थितियों में, पीआईआई को अन्य स्थानों पर पुनर्निर्देशित किया जा सकता है और दुर्भावनापूर्ण गतिविधियों के लिए उपयोग किया जा सकता है।

यही नहीं इससे ग्राहक प्रभावित होता है। डेटा को पुनर्प्राप्त करने का प्रयास करते समय यह बैंक को बहुत परेशान करता है। जब इसे बंधक बना लिया जाता है, तो बैंक को सूचना जारी करने के लिए सैकड़ों हजारों डॉलर का भुगतान करना पड़ सकता है। बदले में, वे अपने ग्राहकों और अन्य वित्तीय संस्थानों का विश्वास खो देते हैं।

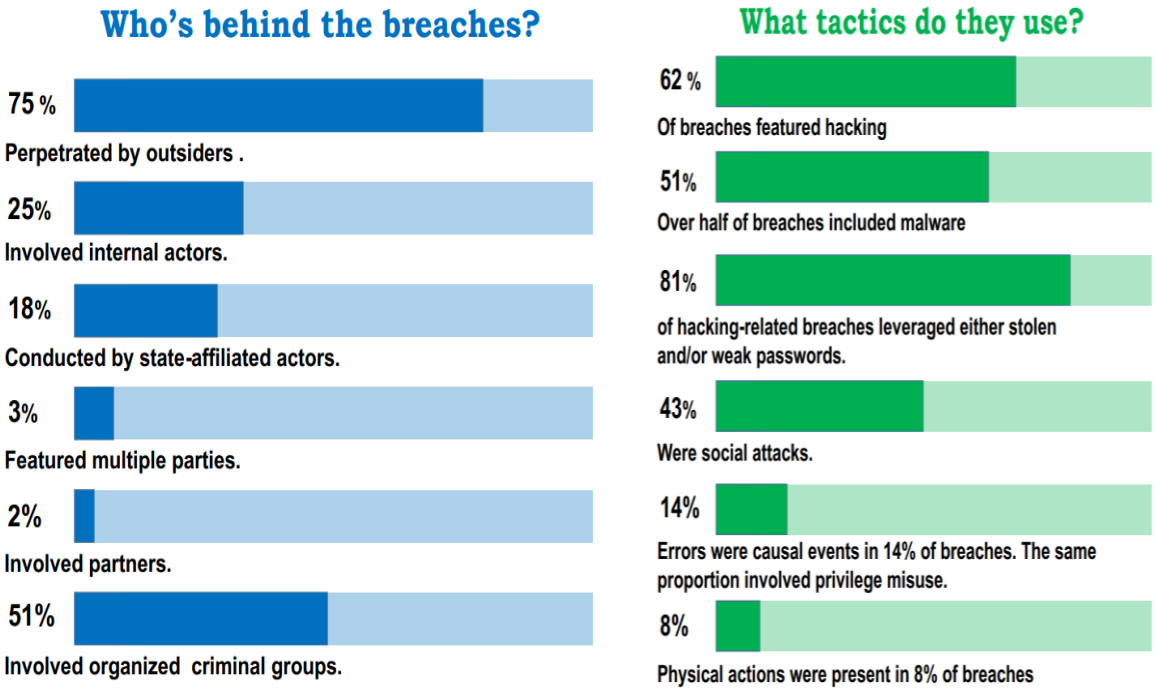
Data Breach से वित्तीय संस्थानों पर भरोसा करना मुश्किल हो सकता है। बैंकों के लिए यह एक गंभीर समस्या है। जब बैंक में Data Breach होता है, तो आप अक्सर समय और पैसा खो देते हैं। इस तरह हुए नुकसान क्षतिपूर्ति कर लेना बेहद कठिन एवं जटिल प्रक्रिया है. अतः आवश्यक है कि

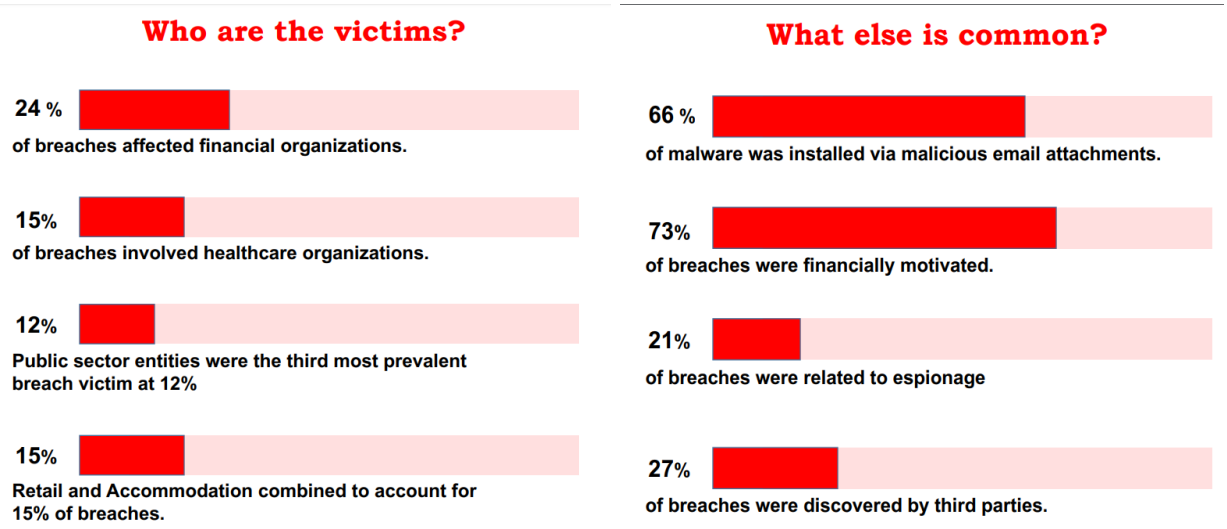
**बैंक एक सुदृण और प्रभावशाली साइबर सुरक्षा पॉलिसी अंगीकार करते हुए अपने इनफार्मेशन एसेट्स को सुरक्षित रखे।**

**जोखिम की वजह से साइबर सिक्युरिटी एक सतत प्रक्रिया है। साइबर-हमलों की बढ़ती मात्रा और जटिलता को विफल करने के प्रयास में सिक्युरिटी सिस्टम को लगातार अपडेट किया जाता है।**

**<u>i) Data Breach डेटा उल्लंघनों की लागत बढ़ रही है:</u>**

**अब लागू होने वाले** EU GDPR (**जनरल डेटा प्रोटेक्शन रेगुलेशन**) **के साथ, आर्गेनाइजेशन्स को कुछ उल्लंघन के लिए** 20 **मिलियन यूरो या वार्षिक वैश्विक कारोबार का** 4% **तक जुर्माने का सामना करना पड़ सकता है। इस पर विचार करने के लिए गैर-वित्तीय लागत भी है, जैसे कि प्रतिष्ठित क्षति और ग्राहक विश्वास की हानि।**






**ii) साइबर हमले तेजी से परिष्कृत होते जा रहे हैं:**

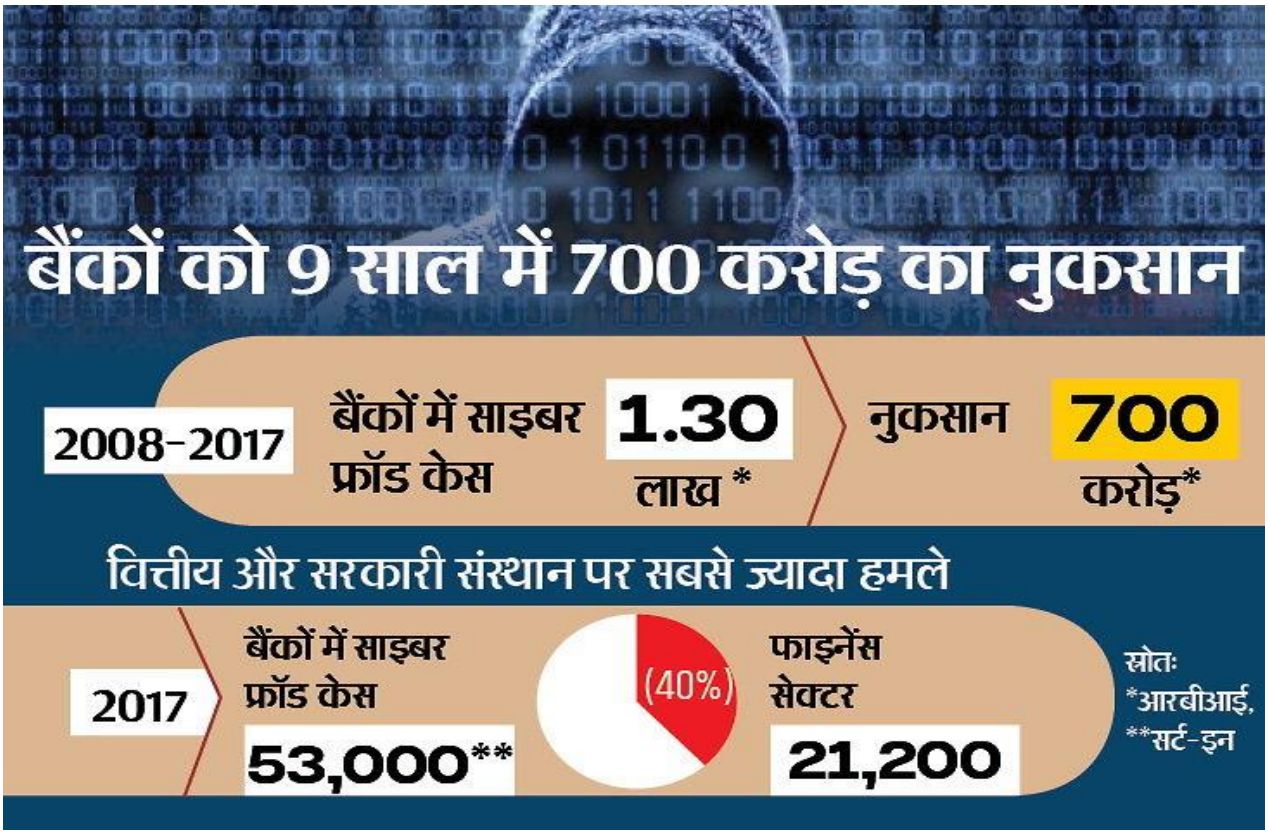
सोशल इंजीनियरिंग, मालवेयर और रैंसमवेयर (जैसा कि पेट्या, वॉन्सेरी और नोटपेटिया के मामले में था) में कमजोरियों का फायदा उठाने के लिए कभी-कभी बढ़ती रणनीति का उपयोग करके हमलावरों के साथ साइबर हमले अधिक परिष्कृत हो गए हैं।

**निष्कर्ष के तौर पर निम्नलिखित कारण हैं कि बैंकिंग में साइबर सुरक्षा महत्वपूर्ण है -**

- डिजिटलाइजेशन की लहर: इन दिनों, सरकार चल रहे डिजिटल पर जोर दे रही है। इसका मतलब है कि जनसंख्या में वृद्धि जो डिजिटल पैसे जैसे प्लास्टिक कार्ड का उपयोग कर रही है और कैशलेस हो रही है। इसलिए, एहतियाती उपायों को लागू करना महत्वपूर्ण हो जाता है जो आपके डेटा और गोपनीयता की सुरक्षा के लिए साइबर सुरक्षा सुनिश्चित करते हैं।
- डेटा ब्रीच से विश्वास का उल्लंघन होता है: डेटा उल्लंघनों से ग्राहकों के लिए वित्तीय संस्थानों पर भरोसा करना मुश्किल हो जाता है। बैंकों के लिए, यह एक गंभीर समस्या है क्योंकि कमजोर साइबर सुरक्षा प्रणाली डेटा उल्लंघनों का कारण बन सकती है।
- वित्तीय घाटा: जब कोई बैंक साइबर हमले से पीड़ित होता है, न केवल बैंक, बल्कि उसके ग्राहक भी वित्तीय नुकसान से पीड़ित होते हैं। इस नुकसान से उबरने में समय लग सकता है। इसमें कार्ड रद्द करना, बयानों की जांच करना और साथ ही अन्य मिनटों की जानकारी की पुष्टि करना शामिल होगा।
- आपका डेटा अब आपका नहीं है: जब साइबर हमलावर एक बार आपके निजी डेटा पर पकड़ प्राप्त करते हैं तो साइबर सुरक्षा बेहद महत्वपूर्ण है; इसका किसी भी तरीके से दुरुपयोग किया जा सकता है। आपका डेटा संवेदनशील है और हमलावरों द्वारा लीवरेज किए जाने के बारे में बहुत सारी जानकारी प्रकट कर सकता है।

# A-फाइनेंस सेक्टर में साइबर हमले

**फाइनेंस सेक्टर में साइबर हमले** 3 **गुना बढ़े, बैंकों को हर साल** 1.50 **लाख करोड़ रु. का नुकसान (**Nov 2018**)**




- **इंटरनेशनल ट्रांसफर के लिए इस्तेमाल होने वाले स्विफ्ट सिस्टम के जरिए सेंधमारी बढ़ी**
- **सिक्योरिटी पर कम खर्च साइबर हमलों की सबसे बड़ी वजह**
- **साइबर फ्रॉड के 40% मामले बैंक और वित्तीय संस्थानों में**

**साइबर हमलों से निपटने के मामले में भारतीय बैंकों का सुरक्षा सिस्टम पुख्ता नहीं है। बैंकिंग सिस्टम में सेंधमारी कर बड़ी रकम साफ करने के तीन बड़े मामले इसी साल सामने आ चुके हैं। इनमें यूनियन बैंक, सिटी यूनियन बैंक, कॉसमॉस बैंक के बाद स्टेट बैंक ऑफ मॉरिशस का मामला भी जुड़ गया। इन सभी बैंकों से हैकर्स ने कुल** 1518 **करोड़ रुपए उड़ा लिए। इस रकम का बड़ा हिस्सा रिकवर हो गया। फिर भी बैंकों को नुकसान उठाना पड़ा।**

पीडब्ल्यूसी और एसोचैम की एक रिपोर्ट के मुताबिक साइबर हमलों और फ्रॉड की वजह से बड़े बैंकों को सालाना 20 अरब डॉलर यानी 1.50 लाख करोड़ रुपए का नुकसान उठाना पड़ता है। दुनिया के फाइनेंस सेक्टर में बीते पांच साल में साइबर हमले 3 गुना तक बढ़े हैं।

## विदेशी बैंकों का साइबर सुरक्षा पर खर्च 10%, भारतीय बैंकों का सिर्फ 4%

1. देश में बड़े बैंक अपने इंफॉर्मेशन और टेक्नोलॉजी (आईटी) बजट का 4 फीसदी हिस्सा साइबर सुरक्षा पर खर्च करते हैं। वहीं, अमेरिका और यूरोप के बैंक अपने आईटी बजट का 6 से 10 फीसदी हिस्सा साइबर सेफ्टी और हैकिंग की चुनौतियों से निपटने की रणनीति बनाने और समाधान खोजने पर खर्च करते हैं।
   कंसल्टिंग फर्म डेलॉय के मुंजल कामदर के मुताबिक साइबर क्राइम के मामले सालाना 10 से 12 फीसदी की दर से बढ़े हैं। इन मामलों में भी बैंकिंग, फाइनेंस और इंश्योरेंस सेक्टर के मामले सबसे ज्यादा हैं। बैंकिंग सेक्टर में सबसे बड़ा खतरा छोटे बैंकों को है। देश में करीब 2000 छोटे बैंक हैं। इनमें को-ऑपरेटिव, डिस्ट्रिक्ट सेंट्रल को-ऑपरेटिव बैंक, क्षेत्रीय ग्रामीण बैंक और स्मॉल फाइनेंस बैंक शामिल हैं। ज्यादातर बैंकों के पास मजबूत साइबर सुरक्षा तंत्र की कमी है।

2.

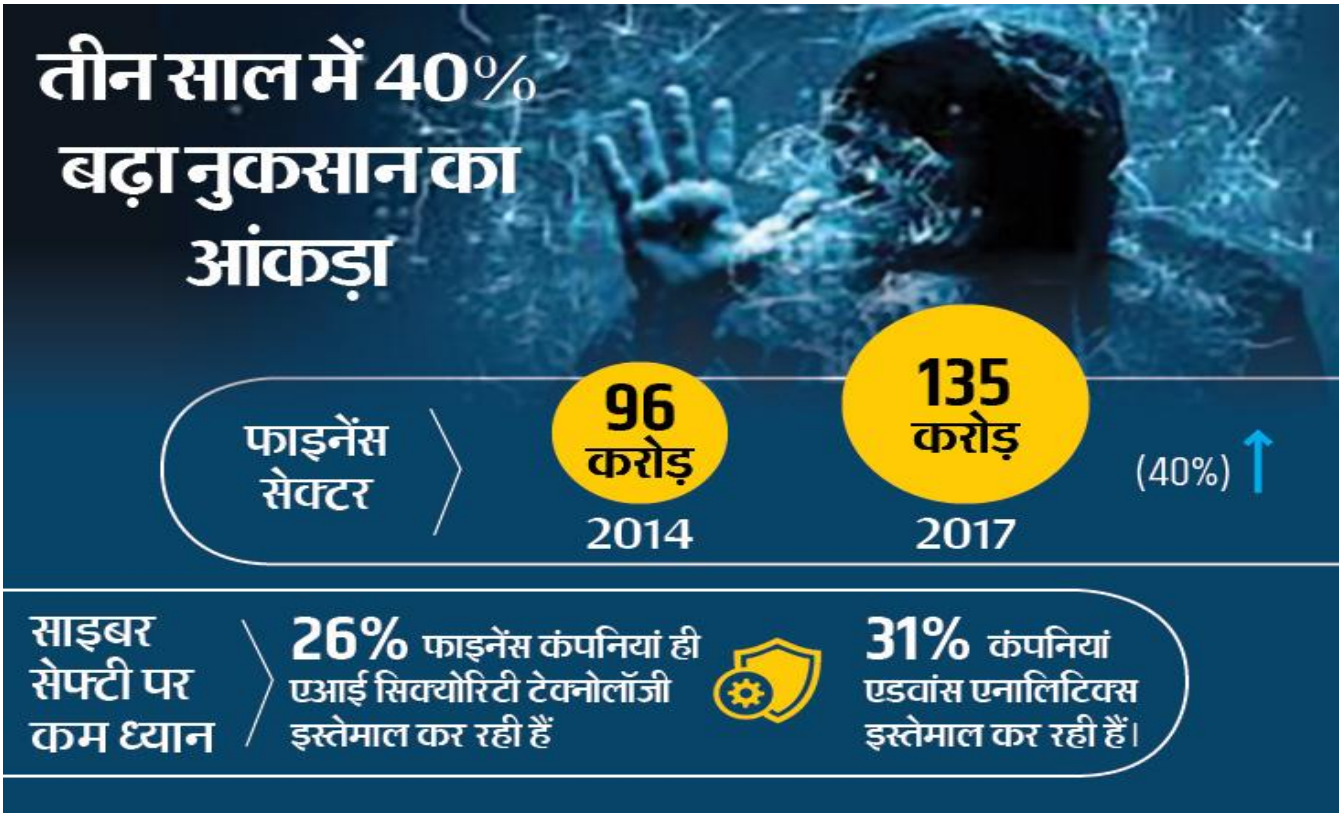
| बैंक | वर्ष | पैसा निकला | वापस नहीं मिला |
|---|---|---|---|
| बैंको डेल ऑस्ट्रो (इक्वाडोर) | 2015 | 90 करोड़ रुपए | 69.34 करोड़ रुपए |
| बांग्लादेश सेंट्रल बैंक | 2016 | 597 करोड़ रुपए | 486 करोड़ रुपए |
| यूनियन बैंक ऑफ इंडिया | 2016 | 1100 करोड़ रुपए | - |
| टीपी बैंक (वियतनाम) | 2016 | 7.37 करोड़ रुपए | - |
| अकबैंक (तुर्की) | 2016 | 29.50 करोड़ रुपए | 29.50 करोड़ रुपए |
| एफईआई बैंक (ताइवान) | 2017 | 422 करोड़ रुपए | 3.68 करोड़ रुपए |
| एनआईसी एशिया बैंक | 2017 | 32.45 करोड़ रुपए | 4.42 करोड़ रुपए |
| ग्लोबेक्स (रूस) | 2017 | 7.37 करोड़ रुपए | 73.76 लाख रुपए |
| सिटी यूनियन बैंक (भारत) | 2018 | 15 करोड़ रुपए | 7.36 करोड़ रुपए |

| | | | |
|---|---|---|---|
| **कॉसमॉस बैंक (भारत)** | 2018 | 95 **करोड़ रुपए** | - |
| **स्टेट बैंक ऑफ मॉरिशस** | 2018 | 143 **करोड़ रुपए** | 14.3 **करोड़ रुपए** |

***(स्रोतः आईएमएफ वर्किंग पेपर, मीडिया रिपोर्ट्स)***

## 3. स्विफ्ट सिस्टम पर बढ़े हमले

**बीते तीन साल में भारत समेत दुनिया में बैंकों के स्विफ्ट सिस्टम को हैक कर बैंकों के डॉलर अकाउंट से पैसा उड़ाने के मामले बढ़े हैं। स्विफ्ट (सोसायटी फॉर वर्ल्ड वाइड इंटरबैंक फाइनेंशियल टेलिकम्यूनिकेशन) सिस्टम एक देश के बैंक को दुनिया के बैंकों से जोड़ता है। इसी के जरिए बैंकों के बीच अंतरराष्ट्रीय स्तर पर पैसा ट्रांसफर होता है। एक साल में भारत के चार बैंकों के स्विफ्ट सिस्टम में सेंध लगाकर हैकर्स ने 1518 करोड़ रुपए साफ कर दिए।**



## 4. 5 साल में 3 गुना बढ़े फाइनेंस सेक्टर में साइबर हमले

**डेटा प्रोटेक्शन और सिक्योरिटी रिसर्च के मामले के प्रमुख संस्थान पोनेमॉन रिसर्च इंस्टीट्यूट और एक्सेंचर की एक रिपोर्ट के मुताबिक दुनियाभर में फाइनेंस सेक्टर में साइबर अटैक के केस पिछले 5 साल में 3 गुना तक बढ़े हैं। 2012 में प्रति कंपनी ऐसे मामलों की संख्या 40 थी, जो 2017 तक 125 पर पहुंच गई। इन हमलों में होने वाला वित्तीय नुकसान 40 फीसदी तक बढ़ा है। रिपोर्ट के मुताबिक 2014 में साइबर हमलों की वजह से दुनियाभर में फाइनेंस सेक्टर में प्रति कंपनी सालाना नुकसान का आंकड़ा 96 करोड़ रुपए था, जो 2017 में बढ़कर 135 करोड़ रुपए पर पहुंच गया। वहीं बाकी सेक्टरों में नुकसान की यही दर 86 करोड़ रुपए है।**


## 5. 60% से ज्यादा साइबर अटैक के पीछे कंपनी से जुड़े लोग

**टेक्नोलॉजी कंपनी आईबीएम की एक रिपोर्ट के मुताबिक साइबर फ्रॉड के 60 फीसदी से ज्यादा मामलों में इनसाइडर की प्रमुख भूमिका होती है। इनसाइडर से मतलब उन लोगों से है जो सीधे या फिर किसी भी तरह से उस फर्म से जुड़े होते हैं। इनमें कंपनी के कर्मचारी, थर्ड पार्टी कान्ट्रैक्टर या फिर बिजनेस पार्टनर भी शामिल होते हैं। हालांकि ज्यादातर मामलों में ऐसे लोगों की प्रत्यक्ष भूमिका नहीं होती।**

**Credits: Dainik Bhaskar**

# B-हैकर्स ने पुणे के Cosmos बैंक में की सेंधमारी, चुराए 92 करोड़

**फिल्मी स्टाइल में की गई यह अब तक की सबसे बड़ी और बेहद अनोखी डीजिटल डकैती है. हैकर्स ने बस एक कमरे में बैठकर कॉसमॉस बैंक के हेड ऑफिस का सर्वर हैक किया और 94 करोड़ रुपये चुरा लिए.**

---

**पुणे के कॉसमॉस बैंक के सर्वर में हैकर्स ने सेंधमारी कर 92.42 करोड़ रुपये चुराने का सनसनीखेज़ मामला सामने आया है. बेहद फिल्मी स्टाइल में की गई यह अब तक की सबसे बड़ी और बेहद अनोखी डीजिटल डकैती है. हैकर्स ने बस एक कमरे में बैठकर कॉसमॉस बैंक के हेड ऑफिस का सर्वर हैक किया और 94 करोड़ गायब हो गए. जांच में पता चला कि 21 देशों के अलग-अलग शहरों के एटीएम से ये 94 करोड़ रुपये निकाले गए हैं.**

**देश के इतिहास में हुई इस सबसे बड़ी बैंक डकैती को लेकर कॉसमॉस बैंक के चेयरमैन मिलिंद काले बताते हैं, 'हैकर्स ने हमारे सर्वर को हैक कर 94 करोड़ों रुपये निकाल लिए. हमारी जांच में पता चला कि 21 देशों से ये पैसे निकाले गए हैं.' हालांकि इसके साथ ही उन्होंने भरोसा दिलाया कि सभी ग्राहकों के पैसे सुरक्षित हैं.**

**वहीं जानकारों का मानना है कि इस तरह की डीजिटल डकैती अपने-आप में अनोखी है. जब भी किसी बैंक के सर्वर में सेंधमारी होती है, तो बैंक के आला अधिकारियों को तुरंत इसकी जानकारी लग जाती है. लेकिन इस मामले में बैंक के अधिकारियों को लंबे समय तक भनक तक नहीं लगी.**

**साइबर क्राइम एक्सपर्ट प्रशांत माली कहते हैं, 'बैंक के सर्वर में सेंधमारी कर ATM को हैक करके बारह हजार ट्रांजैक्शन के जरिये लगभग 94.2 करोड़ रुपये निकाले गए. यह अपने आप में चौंकाने वाली बात है कि इतनी बार ट्रांजैक्शन होने के बावजूद बैंक अधिकारी हरकत में क्यों नहीं आए.' इसके साथ ही वह कहते हैं कि इस घटना से बैंक के ग्राहकों को डरने की जरूरत नहीं है. अगर पुलिस ने वक्त रहते उस पैसे को फ्रीज़ कर दिया है और वह पैसा भारत में रह गया है तो उसके वापस मिलने की संभावना काफी मजबूत है.**

**बैंक की शिकायत पर पुलिस ने इस संबंध में अज्ञात हैकर्स और एएलएम ट्रेडिंग लिमिटेड और हैंगसैंग बैंक के खिलाफ केस दर्ज किया है. पुलिस जांच में पता चला है कि बैंक से चुराए गए 94 करोड़ में से 78 करोड़ रुपये हॉन्ग-कॉन्ग समेत दूसरे विदेशी शहरों से निकाले गए हैं, जबकि बाकी के 14 करोड़ भारत में ही अलग-अलग शहरों के एटीएम से निकाले गए. Credits-News18**

# C-Lessons from the Cosmos Bank attack

In August this year, Cosmos Bank became the latest victim of a major cyber-attack. Hackers breached the bank's ATM switch server in Pune, stealing details of multiple Visa and Rupay debit card owners. The details were then used to carry out around 12,000 fraudulent transactions across 28 countries on August 11 – with a further 2,841 transactions taking place in India.

The attack didn't stop here. Two days later, on August 13th, in another malware attack on the bank's server, a SWIFT transaction was initiated – transferring funds to the account of ALM Trading Limited in Hanseng Bank, Hong Kong.

The total losses from the attack stand at INR 94 crore, or 13.5 million USD. Cosmos Bank was forced to close its ATM operations and suspend online and mobile banking facilities.

**How did the attack happen?**

- Malware attack: The core banking system (CBS) of the bank receives debit card payment requests via a 'switching system'. During the malware attack, a proxy switch was created and all the fraudulent payment approvals were passed by the proxy switching system.
- ATMs compromised: When depositors withdraw money at ATMs, a request is transferred to the respective bank's CBS. If the account has sufficient balance, the CBS will allow the transaction. In the case of Cosmos Bank, the malware created a proxy system that bypassed the CBS. While cloning the cards and using a 'parallel' or proxy switch system, the hackers were able to approve the requests – withdrawing over INR 80.5 crore in approximately 15,000 transactions.
- Reserve Bank of India (RBI) guidelines: RBI has clear guidelines to protect against incidents such as the Cosmos Bank attack which must be followed. The security measures across Indian banks are moderate and given the high level of coordinated international attacks, all banks need to upgrade their security mechanisms.

**Why is this attack more serious?**

Just a few days prior to this attack, the American FBI had warned banks of a major hacking threat to ATMs worldwide. According to Krebs On Security, the influential cyber-security blog run by journalist Brian Krebs, a confidential alert to international banks informed them that criminals were plotting an imminent, concerted global malware attack on ATMs.

Smaller banks with less sophisticated security systems were believed to be most vulnerable to attack – with a scheme known as 'ATM cash-out' as the likely approach that the criminals might take. This is where crooks hack a bank or payment card processor and use cloned cards at ATMs around the world to fraudulently withdraw millions of dollars in just a few hours.

Banking experts and industry players fear this could be a 'pilot run' unless the authorities take the attack seriously. Essentially, this malware attack was not against any bank but rather, the banking system. It was carried out at international scale in a meticulously coordinated manner.

**Alert type – Severe**

**How can I protect my enterprise?**

To defend your company from the spread of malware, it's essential that you are equipped to detect and defeat such threat in real-time.

These are our recommended immediate best practices:

1. Back up data regularly – verifying data integrity and testing the restoration process
2. Secure your offline backups – ensuring backups are not connected permanently to the computers and networks they're backing up on
3. Audit firewalls, servers and Intrusion Prevention System (IPS) configurations – block access to known malicious IP addresses & Server Message Block (SMB) ports 139 and 445, and disable SMBV1 and Windows Management Instrumentation Command Line (WMIC) in servers and Active Directory (AD)
4. Patch operating systems, software and firmware on devices – use a centralised patch-management system
5. Scan all incoming and outgoing emails – detect threats and filter executable files from reaching end users using sandboxing
6. Enable strong spam filters to prevent phishing emails – authenticate inbound email using technologies such as Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) to prevent spoofing

**Be prepared**

Enterprises need to ensure that security is inbuilt end-to-end – starting at the very beginning. Protecting your network should be the #1 priority to safely extend your reach virtually anywhere. Solutions such as our Managed Security Services offer 24/7/365 security.

**Credits:** **Rajarshi Purkayastha**, Head, Pre-Sales, India and MECAA, Tata Communications

## 2.3 आईटी प्रोडक्ट सम्बंधित सावधानियाँ साइबर सुरक्षा के फायदे

# Do's & Don'ts of IT Products

**Any Body Can Do Information Security**
**Safety Comes with Responsibility**

## Do's and Don'ts while Browsing

Do's

- Install and use a firewall, pop-up blocker and spyware detector. Maintain the logs.
- Ensure that Anti-Virus is installed and up to date.
- Run anti-virus and spyware detectors/cleaners regularly.
- Habitually download security protection update patches & Keep your browser and operating system up to date.
- Make Backups of Important Files and Folders.
- Use strong passwords (alphanumeric and special characters) - Easy to remember and difficult to guess. Change administrator' default password.
- Use a variety of passwords, not same for all of your account.
- Disconnect internet connection when not in use.
- Make the wireless network invisible by disabling identifier broadcasting. If the wireless network does not have a default password, create one and use it to protect the network.
- Disable file sharing on computers.
- Avoid online banking, shopping, entering credit card details, etc if the network is not properly secured.
- Check your online account frequently and make sure all listed transactions are valid.
- Be extremely wary of spam legitimate looking email asking for confidential information. Never ever click on the link given in the spam email.
- Always delete spam emails immediately and empty the trash box to prevent accidental clicking on the same link.
- Be wary of websites that require your card details up front before you actually place an order.
- Never respond to text messages from someone you don't know.
- Open email attachment carefully.
- Be careful while downloading any free software or screensaver etc.
- Not delete email in question, save the email and take out the full header of the such email and report the crime.
- Be cautious when dealing with individuals not known to you or outside of your own country.
- Be cautious of unsolicited offers. Never purchase anything advertised through an unsolicited email.

- Beware of promises to make fast profits. Be cautious of exaggerated claims of possible earnings or profits.
- Beware of lotteries that charge a fee prior to delivery of your prize.
- Always type website addresses yourself rather than clicking on a link provided.

Don’s

- Expose yourself that you are not available in town or give your details about location and itinerary when email auto responder enabled.
- Hand over your credit card to any person.
- Auto-connect to open Wi-Fi (wireless fidelity) networks
- Get confused, frightened or pressured into divulging information if you receive an e-mail purporting to be from your bank or credit card provider as criminal use scare tactics.
- keep passwords stored on your computer.
- To go online without virus protection and a firewall in place.
- Open email attachment if you are not sure about it.
- Provide any information like Your real name, home address, your phone number, your friends' or family members' private information, your passwords to anonymous chat friend
- Always keep your cards in safe and secured place.
- Always make sure contact numbers of your bank is readily available with you. Take diary note of your card numbers for any time reference.
- Always keep the card’s safe by Memorising. Choose a strong safe PIN code, which is not easy to guess. Change the PIN number frequently.
- If anything makes you uncomfortable during the ATM transaction, hit the cancel button.
- Always request for a receipt of a transaction.
- Be especially cautious using ATMs at night. If the machine is poorly lit avoid it.
-

**Do’s and Don’ts for Credit / ATM cum Debit Card**

Do’s

- Observe the ATM site and make sure no one is lingering nearby. Cover the keypad while keying in your PIN.
- Always leave the ATM only after the transaction is fully completed.
- Always ensure the card is swiped in front of you at all times.
- Always register your mobile number at the branch to get SMS alerts.
- Always inform for change of address to the Bank promptly.
- Always follow the guidelines which are issued by Bank.

Don’ts

- Don’t accept the card if it is damaged.

- Don't expose the card to excessive heat or keep close to a magnetic field.
- Don’t list the PIN on your Debit or Credit card.
- Don’t disclose your Card PIN to anyone.
- Don’t carry around extra credit cards that you rarely use.
- Don’t hand over the card to anyone, even if He / She claims to represent the Bank.
- Don’t take help from strangers while using ATM Machine.

## Do’s and Don’ts for Internet Banking

Do’s

- Always keep your Internet banking password and transaction password secret.
- Always keep a unique password and keep changing it regularly.
- Always set password that is easy to remember but difficult to guess.
- Ensure that no one is watching you when you are entering password.
- Always use Virtual keyboard for typing user id and password.
- Always check website address of your bank before login.
- Always click the padlock on the status bar and ensure that it has valid certificate pertaining to your bank.
- Check your account statement regularly.
- Refrain from accessing your bank account at public places like cyber café.
- Always update your web browser and enable phishing filter.
- Always ensure that your computer has Antivirus and Anti Spyware installed and it is updated.
- Log off completely from your on-line banking website, close the browser and log off your PC, when not in use.
- Follow our advice and guidelines given on our website.

Don’ts

- Never disclose internet banking username, password, on phone call or email.
- Never leave the PC unattended while using internet banking.
- Don’t open multiple tabs in your brows long time.
- Don’t reply to an Email or Pop-up message that ask for personal information like password, login to Internet Banking or PIN. Bank will never demand such sensitive information. You may call the bank to know the factual position.
- Never download/install/run programs/files from untrusted sources.
- Don’t click on any link which has come through unknown sources.
- Don’t access the Internet Banking website through a link from another web site or a link in an E-mail.
- In case you smell anything fishy, call and confirm from our Bank before you act as requested.

## Do’s and Don’ts  for Mobile Banking

Do’s

- Set up a strong Pin/password to access the handset menu on your mobile phone.
- Change Mobile Banking Pin/ Transaction Password periodically.
- Register for SMS alerts to keep track of your banking transactions.
- Install an effective mobile anti-malware/anti-virus software on your smartphone and keep it updated.
- Keep your mobile's operating system and applications, including the browser, updated with the latest security patches and upgrades.
- Clear temporary files stored in the memory as they may contain your sensitive information when you send your mobile for repair/maintenance.
- Turn off wireless device services such as Wi-Fi and Bluetooth, when they are not being used.
- Log out from online mobile banking or application as soon as you have completed your transactions. Also make sure you close that window.
- Contact Bank in case of loss/theft of mobile device for blocking the mobile banking services.

Don’ts

- Don't open every SMS / MMS as it may contain viruses, especially from unknown sources.
- Do not save confidential information such as your debit/credit card numbers, CVV2 numbers or PINs on your mobile phone.
- Never accept offers such as caller tunes or dialer tunes from unknown sources.
- Be careful about the websites you are browsing. If it does not sound authentic, do not download anything from it.
- Never connect your mobile phone through an unsecured Wi-Fi connection available in public places such as airports etc.

## साइबर सुरक्षा के फायदे (Advantages of Cyber Security)

साइबर सुरक्षा इसलिए जरूरी है क्योंकि सरकार, मिल्टरी, कॉर्पोरेट, फाइनेंशियल और मेडिकल संस्था काफी तरह के डाटा को इक्कठा करता है और उस डाटा को अपने सिस्टम, कम्प्युटर और अन्य उपकरणों में रखता है। इस डाटा का कुछ भाग काफी महत्वपूर्ण भी हो सकता है जिसके चोरी होने से किसी की निजी ज़िंदगी पर काफी गहरा प्रभाव पड़ सकता है और इससे उस संस्था की सारी मिट्टी पलित हो सकती है।

साइबर सुरक्षा की मदद से इस ढेरो डाटा को सुरक्षित रखा जाता है जिससे की यह डाटा किसी और के हाथ नहीं लग सके। जैसे जैसे डाटा बढ़ता जाता है वैसे वैसे हमें अच्छे और प्रभावशाली साइबर सुरक्षा के उत्पादों और सर्विसों की जरूरत पड़ती है।

साइबर सुरक्षा की मदद से हम साइबर हमले, डाटा की चोरी और चोरों की धमकी से बच सकते हैं। जब भी किसी संस्था में किसी अच्छे तरह के नेटवर्क की सुरक्षा होती है और किसी भी तरह की मुश्किल से बचने के तरीके होते हैं यह सब काम साइबर सुरक्षा के उत्पादों और सर्विसों की मदद से ही मुमकिन हो पाता है। उदाहरण के लिए काफी तरह के एंटिवाइरस आदि हमें वाइरस के हमलों से बचाते हैं।

# साइबर हमले

## 3.1 साइबर हमलों के प्रकार (Types of Cyber attacks)

साइबर अपराध ऐसे गैर-कानूनी कार्य हैं जिनमें कंप्यूटर एवं इंटरनेट नेटवर्क का प्रयोग एक साधन अथवा लक्ष्य अथवा दोनों के रूप में किया जाता है।

बदलती तकनीकी की वजह से हमारी सुरक्षा और थ्रेट इंटेलिजेंस हमारे लिए काफी चुनौती भरा काम हो गया है। हालांकि साइबर धमकियों से बचने के लिए हमें हमारी जानकारी को सुरक्षित रखना काफी जरूरी है।

- मालवेएर (Malware)- यह कम्प्युटर की किसी फाइल या फिर प्रोग्राम को नुकसान पहूँचाती है जैसे की कम्प्युटर वाइरस, वोर्म, ट्रोजन आदि।

  वायरस (Virus) वायरस एक प्रकार के मैलवेयर प्रोग्राम हैं जिन्हें विशेष रूप से पीड़ितों के कंप्यूटर को नुकसान पहुंचाने के लिए डिज़ाइन किया गया है। वायरस सही परिस्थितियों में आत्म-प्रतिकृति कर सकते हैं और यूजर की अनुमति या ज्ञान के बिना कंप्यूटर सिस्टम को संक्रमित कर सकते हैं।

  रेनसमवेएर (Ransomware)- यह एक तरह का वाइरस होता है जो की अपराधी द्वारा लोगों के कम्प्युटर और सिस्टमों में हमला करने के लिए काम में आता है। यह कम्प्युटर में पड़ी फाइलो को काफी नुकसान पहूँचाता है। फिर उसके बाद अपराधी ने जिस किसी का भी कम्प्युटर या सिस्टम इस तरीके से खराब किया होता है उससे रिश्वत लेता है और उसी के बाद उसके सिस्टम को छोड़ता है।

  ट्रोजन(Trojen) एक प्रकार के मैलवेयर प्रोग्राम हैं जो स्वयं को हानिरहित या उपयोगी सॉफ़्टवेयर के रूप में प्रस्तुत करते हैं। ट्रोजन पीड़ितों के कंप्यूटर पर दुर्भावनापूर्ण प्रोग्राम डाउनलोड करने, फ़ाइलों को डिलिट करने या चोरी करने और हैकर्स के लिए पीड़ितों के कंप्यूटर पर अनधिकृत एक्सेस प्रदान करने सहित कई प्रकार की दुर्भावनापूर्ण गतिविधियों का कारण बन सकते हैं।

  एडवेयर(Adware) मैलवेयर का एक समूह है जो पॉप-अप को उत्पन्न करने के लिए जाना जाता है।

यदि यूजर उस अतिरिक्त सॉफ़्टवेयर को डाउनलोड करता है, तो वह आपके डेटा को या तो डिलिट कर सकता है या चोरी कर सकता है। इन पॉप-अप मैसेज में से कुछ का उपयोग आपके कंप्यूटर स्क्रीन को केवल अवांछित जानकारी जैसे विज्ञापनों के साथ Cyber बम बनाने के लिए भी किया जा सकता है।

- **Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks**: मतलब किसी सर्विस को देने से इंकार करना। Dos Attack में हैकर किसी website/network को टारगेट बनाता है और ,इतनी ज्यादा fake ट्रैफिक generate करता है की वेबसाइट/नेटवर्क उस ट्रैफिक को हैंडल नहीं कर पता है और आख़िरकार बंद हो जाता है। ऐसे में उस वेबसाइट के जितने भी रियल user होते हैं वे भी वेबसाइट पे available डाटा को access नहीं कर पाते हैं।

  हर वेबसाइट या सर्वर का एक लिमिट होता है की वो एक टाइम में ज्यादा से ज्यादा कितने users को हैंडल कर सकता है ,लेकिन ये अटैक ऐसा होता है जिसमे लगातार बहुत ज्यादा ट्रैफिक generate होती है और जिसके वजह से सर्वर स्लो हो जाता है और कई बार क्रैश भी।

  DDOS का फुल फॉर्म होता है Distributed denial of service . ये भी DOS अटैक ही है लेकिन ये डिस्ट्रिब्यूटेड अटैक होता है। तो दोस्तों ये थोड़ा अलग है Dos attack से ,क्यूंकि इसमें कोई एक host/system अकेले ही अटैक नहीं करता है है बल्कि बहुत से सिस्टम/कंप्यूटर एक साथ अटैक करते हैं। इस अटैक में सिर्फ एक ही कंप्यूटर यूज़ नहीं होता है। DDOS काफी सोचा समझा और खतरनाक अटैक माना जाता है।

  इस अटैक में हैकर दुनिआ भर के बहुत सारे system को अपने virus से affect करता है और botnet तैयार करता है। या फिर हम ये कह सकते हैं की ये कंप्यूटर जिनमे virus आ जाता है वो उस हैकर के Robot बन जाते हैं और वही करते हैं जो हैकर कहता है। तो हैकर जब botnet बना लेता है तब वो इन systems का यूज़ करके एक साथ किसी टारगेट वेबसाइट पे DDoS attack करता है।

  जैसा की हमने पहले भी जाना सर्वर एक टाइम में एक लिमिट तक ही ट्रैफिक हैंडल कर सकता है, लेकिन DDOS ATTACK में हैकर अपने रोबोट्स को आर्डर देता है और बहुत सारा fake ट्रैफिक generate होता है जिसके वजह से वह वेबसाइट down या पूरी तरह बंद हो जाती है।

- **Password Attacks: यह एक प्रकार का साइबर सिक्युरिटी खतरा है जिसमें यूजर के पासवर्ड को क्रैक करने के लिए हैकर्स द्वारा हैकिंग का प्रयास शामिल है। हैकिंग टूल की सहायता से, हैकर्स पीड़ित के खाते की क्रेडेंशियल्स प्राप्त करने और पहुँच प्राप्त करने के लिए कई पासवर्ड एंटर कर सकते हैं।**

- **सोशल इंजीनियरिंग (Social engineering) - यह एक तरीके का हमला है जो की मनुष्य के वार्तालाप पर निर्भर करता है। जिससे की बड़ी चालाकी से लोगों को जाल में फसाया जा सके और उनसे उनके निजी डाटा, पासवर्ड आदि को निकलवाया जा सके। इस वजह से भी लोगों को काफी खतरा है इसलिए जिस किसी से भी बात करें काफी सोच समझ कर ही करें।**

- **Identity Theft यह एक प्रकार का साइबर सिक्युरिटी खतरा है जिसमें सोशल मीडिया वेबसाइटों जैसे कि फेसबुक, इंस्टाग्राम आदि से पीड़ितों की व्यक्तिगत जानकारी की चोरी करना और पीड़ितों का एक पिक्चर बनाने के लिए उस जानकारी का उपयोग करना शामिल है। यदि पर्याप्त संवेदनशील जानकारी एकत्र की जाती है, तो यह साइबर क्राइम को किसी तरह से आपके जैसे दिखावा करने की अनुमति दे सकता है।**

- **Digital Abuse डिजिटल एब्यूज़ का अभिप्राय टेक्स्टिंग (Texting) और सोशल नेटवर्किंग जैसी तकनीकों का उपयोग किसी को धमकाने, परेशान करने, डाँटने या डराने के लिये किये जाने से है। आमतौर पर यह अपराध ऑनलाइन (Online) किये जाने वाले मौखिक और भावनात्मक दुर्व्यवहार का एक रूप होता है।**

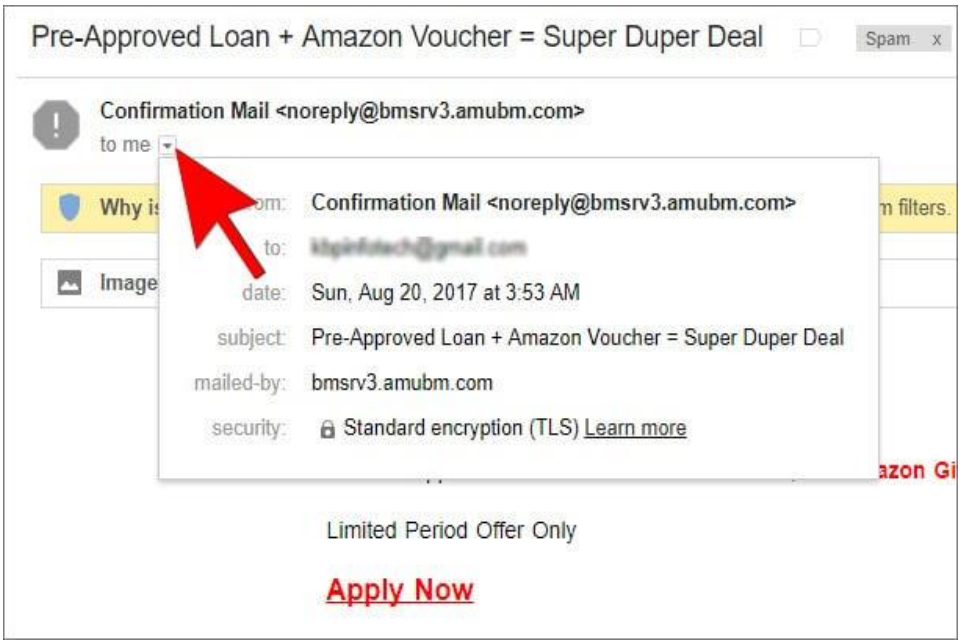
- **Cyberstalking साइबरस्टॉकिंग का तात्पर्य किसी अन्य व्यक्ति से लगातार अवांछित संपर्क स्थापित करना या ऐसा करने की कोशिश करना है, चाहे वह पहचान का हो अथवा अजनबी।**

- **Spyware and Keyloggers (स्पाइवेयर और कीलॉगर) यूजर की इनफॉर्मेशन, पासवर्ड, ब्राउज़िंग हिस्ट्री इत्यादि इकट्ठा करते हैं, और फिर उन्हें अपने क्रिएटर (हैकर्स) तक पहुंचाते हैं, जो इस व्यक्तिगत जानकारी को थर्ड पार्टी को बेचता या वितरित कर सकते हैं। हैकर्स उसका इस्तेमाल पीड़ित के बैंक अकाउंट से पैसे चुराने के लिए भी कर सकते हैं।**

- **फिशिंग (Phishing) Emails-  फ़िशिंग ईमेल का उपयोग आमतौर पर यूजर से निजी जानकारी चुराने के लिए किया जाता है जबकि स्पैम ईमेल का उपयोग आम तौर पर इंटरनेट पर एक ही मैसेज की कई कॉपिज के साथ बाढ़ लाने के लिए किया जाता है, जो कंप्यूटर यूजर को इस मैसेज पर लाने को मजबूर करने के प्रयास होता है जो अन्यथा इसे प्राप्त करने का विकल्प नहीं चुनते हैं।**

**<u>कैसे चेक करें कि कोई ईमेल असली है या नहीं</u>**

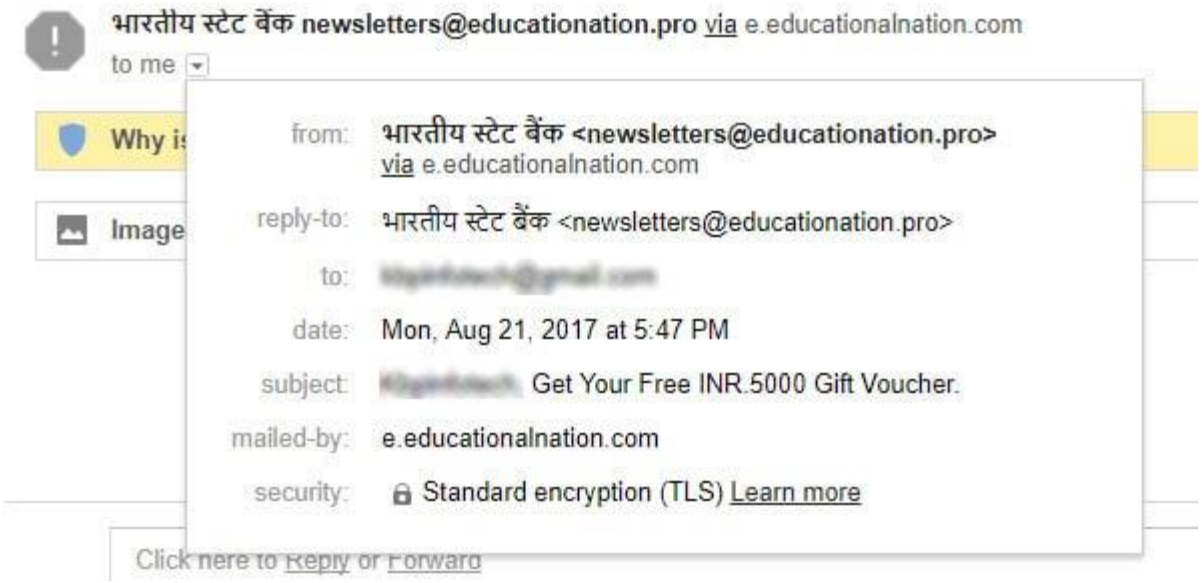
- **ईमेल की विश्वसनीयता को सिध्द करने के लिए, आपको भेजने वाले का ईमेल एड्रेस और ईमेल हेडर को चेक करना होगा।**
  **एक असली और नकली ईमेल के बीच अंतर करने की क्षमता भी आपके ईमेल क्लाइंट पर निर्भर करती है। मैं यह नीचे समझाता हूँ**
- **यदि आपको किसी मेल पर शंका हैं, तो पहले वह मेल ओपन करें।**
- **यदि आप Gmail का उपयोग कर रहे हैं तो जीमेल की स्किल को बढ़ाकर एक्स्पर्ट बन सकते हैं। Gmail में आप आसानी से फेक या रियल मेल चेक करने के लिए भेजने वाले के नाम के नीचे के Show Details ऐरो को क्लिक करें।**




- **इस स्क्रीनशॉट में, आप देख सकते हैं कि ईमेल** noreply@bmsrv3.amubm.com **से भेजा गया हैं।**

- **अब आपको यह चेक करना चाहिए की यह ईमेल सच में** amubm.com **से हैं या नहीं। इस हेडर में** mailed- by, signed-by **और** encryption **इम्पोर्टेन्ट सेक्शन हैं।**

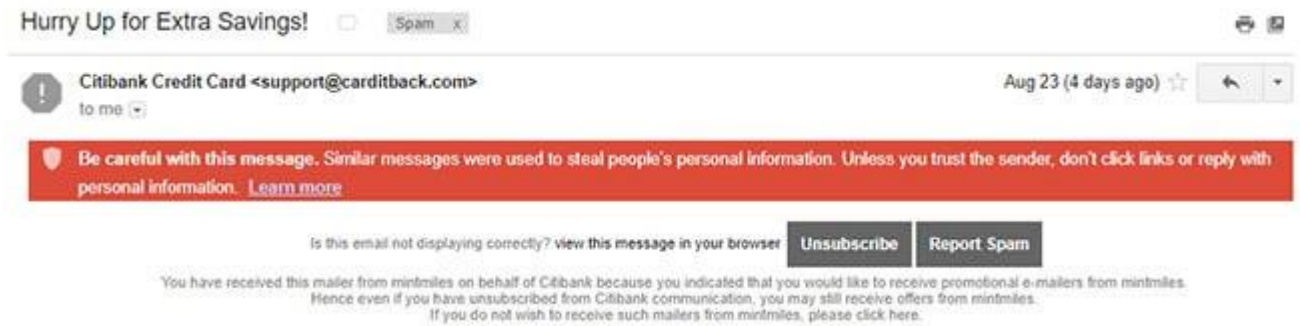
- **इस मेल में** signed-by **फ़ील्ड मिसिंग हैं। ऐसे में इस ई-मेल पर ज़्यादा भरोसा नहीं कर सकते। एक और उदाहरण जो ई-मेल "भारतीय स्टेट बैंक" के नाम से आया दिख रहा है।**




**इसके डिटेल्स चेक करने पर यह ई-मेल** newsletters@educationation.pro **से प्राप्त हुआ हैं।**

- **यहां पर भी** signed-by **फ़ील्ड मिसिंग हैं। किसी बैंक या बड़ी कंपनी से आने वाले मेल में हमेशा** signed-by **फ़ील्ड होना चाहिए।**
  **इसके साथ ही, अगर कोई वास्तव में नकली अन्य ईमेल एड्रेस की कोशिश करता हैं, तो** Google

  **आपको बताता हैं और इस बात की चेतावनी आपको दे सकता है**:




**अगर आपको इस तरह के वॉर्निंग्स के ई-मेल मिलते है, तो आपको इन ईमेल पर भरोसा नहीं करना चाहिए।**

## 3.2 वित्तीय संस्थानों को मुख्य साइबर खतरे (Top Threats to Financial Institutions)

**Financial institutions are advised to avoid these common mistakes that create opportunities for prepared hackers:**

**Unencrypted Data - the majority of data breaches in 2015 were caused by improper encryption, making stolen data immediately accessible after being stolen.**

**New Technology Without Security - CCTV cameras, connected cars, medical devices, and toys can all be turned into bots if they are unprotected. It is important to remember that more than just your computer hard drive data can be compromised and used against you.**

**Third Party Services - The Internet is a natural connector, though unprotected third party services can open the door for cyber attackers to acquire more data. Cybersecurity should be a priority when you connect services, rather than an afterthought.**

**Being Unprepared for New Forms of Hacking - Hackers do not only delete consumer data, they change or hold it hostage for later use. Deleting data is not the only way that a hacker can compromise a financial service.**

**Unsecured Mobile banking - As mobile banking becomes more popular, less complicated security systems on mobile devices present opportunities for expert hackers. Encryption must extend into the mobile space for banks and customers to remain safe.**

## 3.3 साइबर हमलों से रोकथाम

**बैंकिंग क्षेत्र में साइबर सुरक्षा को बढ़ाने के लिए क्या किया जा सकता है?**

- **बैंक नियामकों को तीसरे पक्ष के विक्रेताओं की जांच करने की अनुमति दी जानी चाहिए कि कई क्रेडिट यूनियन इन दिनों प्रौद्योगिकी सेवाओं के लिए उपयोग कर रहे हैं।**
- **डेटा उल्लंघनों और साइबर सुरक्षा की घटनाओं के प्रभाव को कम करने के लिए तीव्र प्रतिक्रिया की आवश्यकता है। इस तरह के साइबर खतरों से बचने के लिए प्रोएक्टिव उपाय अपनाएं।**
- **साइबर अटैक सिम्युलेटर और थ्रेटकॉप जैसे जागरूकता उपकरण के साथ, बैंक कर्मचारी साइबर हमले के विभिन्न रूपों के बारे में जान सकते हैं। यह उपकरण चार-चरण चक्र की सहायता से सुनिश्चित किया गया है। इसमें सिम्युलेटेड हमला, ज्ञान प्रदान करना, एक मूल्यांकन शामिल है, जिसके बाद एक और नकली हमला होता है।**

### सुरक्षित सॉफ्टवेयर के साथ हमलों के खिलाफ सुरक्षा

**जब आप इंटरनेट पर सुरक्षा की चालू स्थिति को देखते हैं, तो आपको अपने वर्तमान सुरक्षा अनुप्रयोगों को बढ़ाने या पूर्ण प्रतिस्थापन पर विचार करना चाहिए। बैंकिंग सॉफ्टवेयर विकास की दुनिया में देखने के लिए यहां कुछ चीजें हैं।**

- **इनफार्मेशन सिक्योरिटी ऑडिट - किसी भी नए साइबर सिक्योरिटी सॉफ्टवेयर को लागू करने से पहले पूरी तरह से ऑडिट जरूरी है। समीक्षा में मौजूदा सेटअप की ताकत और कमजोरियों का पता चलता है। इसके अलावा, यह सिफारिशें प्रदान करता है जो उचित निवेश के लिए अनुमति देते हुए पैसे बचाने में मदद कर सकता है।**
- **फ़ायरवॉल - साइबर सुरक्षा बैंकिंग कॉन्फ़िगरेशन में केवल एप्लिकेशन शामिल नहीं हैं। हमलों को रोकने के लिए सही हार्डवेयर की भी आवश्यकता होती है। एक अद्यतन फ़ायरवॉल के साथ, बैंक नेटवर्क के अन्य हिस्सों तक पहुँचने से पहले दुर्भावनापूर्ण गतिविधि को रोक सकते हैं।**
- **एंटी-वायरस और एंटी-मैलवेयर एप्लिकेशन - जबकि एक फ़ायरवॉल अपग्रेड सुरक्षा बढ़ाता है, यह तब तक हमलों को नहीं रोकेगा जब तक कि एंटी-वायरस और एंटी-मैलवेयर एप्लिकेशन अपडेट न हों। पुराने सॉफ़्टवेयर में नवीनतम नियम और वायरस हस्ताक्षर नहीं हो सकते हैं। बदले में, यह आपके सिस्टम पर संभावित विनाशकारी हमले को याद कर सकता है।**

- मल्टी-फैक्टर ऑथेंटिकेशन - यह सुरक्षा, जिसे एमएफए के रूप में भी जाना जाता है, उन ग्राहकों की सुरक्षा के लिए बेहद महत्वपूर्ण है जो अपने बैंकिंग करने के लिए मोबाइल या ऑनलाइन ऐप का उपयोग करते हैं। कई उपयोगकर्ता अपने पासवर्ड कभी नहीं बदलते हैं। या, यदि वे करते हैं, तो वे छोटे बदलाव करते हैं। एमएफए को लागू करना हमलावरों को नेटवर्क तक पहुंचने से रोकता है क्योंकि यह सुरक्षा के एक और स्तर की मांग करता है। उदाहरण के लिए, ग्राहक के सेल फोन पर भेजा गया छह अंकों का कोड।
- बायोमेट्रिक्स - यह एमएफए का एक और संस्करण है जो टेक्स्टेड कोड की तुलना में अधिक सुरक्षित है। प्रमाणीकरण का यह रूप उपयोगकर्ता की पहचान की पुष्टि करने के लिए रेटिना स्कैन, अंगूठे के निशान या चेहरे की पहचान पर निर्भर करता है। हालांकि हैकर्स ने अतीत में इस प्रकार के प्रमाणीकरण तक पहुंच बनाई है, लेकिन इसे पूरा करना अधिक कठिन है।
- स्वचालित लॉगआउट - कई वेबसाइट और एप्लिकेशन उपयोगकर्ता को लॉग इन रहने की अनुमति देते हैं यदि वे इसे अनुमति देते हैं। इस प्रकार, वे अपनी लॉगिन क्रेडेंशियल दर्ज किए बिना किसी भी समय अपनी जानकारी तक पहुंच सकते हैं। हालाँकि, यह भी हमलावरों को आसानी से आपके रिकॉर्ड प्राप्त करने की अनुमति देता है। निष्क्रियता के कुछ मिनट बाद उपयोगकर्ता की पहुंच को बंद करके स्वचालित लॉगआउट इसे कम कर देता है।
- शिक्षा - उपरोक्त सभी उपाय बैंकिंग क्षेत्र में साइबर सुरक्षा को बढ़ा सकते हैं। फिर भी, यदि ग्राहक असुरक्षित स्थानों से अपनी जानकारी प्राप्त करना जारी रखते हैं या अनुचित तरीके से अपने लॉगिन क्रेडेंशियल्स को सुरक्षित रखते हैं, तो वे मदद नहीं कर सकते। यही कारण है कि शिक्षा महत्वपूर्ण है। जब बैंक अपने ग्राहकों को इन कमजोरियों से संबंधित परिणामों के बारे में सूचित करते हैं, तो यह उनके निवेश को खोने के डर से अपनी आदतों को बदलने के लिए उन्हें स्थानांतरित कर सकता है।

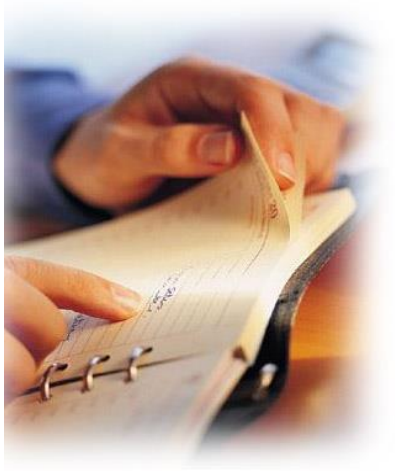
TATA CONSULTANCY SERVICES
Experience certainty.

# Security Features in TCS CBS

23rd November 2019



## Agenda



- Application Security Features
- Reports
- EOD checks
- Password Security

## Security features in application and service model

TCS BaNCS application has the following features to secure the bank's and end users interest

- Front end level validation
- Maker checker concept
- Product level validations
- Customer level validations
- Mandatory fields wherever required
- Various monitoring reports

TCS BaNCS ASP model has standard processes to secure the bank's and end users interest

- User creation
- Parameter changes
- Configuration changes
- Updates and rectifications



## User Management in CBS

- The CBS applications supports various capabilities, groups and user types which can be configured as per Bank's requirement.
- Every user is assigned a user capability, user group and user type during user creation. This is decided by the bank at the time of requesting user creation to help desk.
- The user capability varies from 2 to 9
- User group definition allows the bank to have different users of same capability to have different functions access in CBS
- The menu provided to the user depends on the user type he is assigned

## User Management in CBS

- The user password strength is also defined by the bank user.
- The password strength depends on what combination of alphabets, numbers and special characters is configured by the bank.
- The user is auto locked based on inactive time.
- After lock out, user needs to enter his password again.
- The application also supports biometric login authentication facility where the user's finger scan is captured during login process.



## User Creation and Login in CBS

- User is created only on the basis of request from the bank that is systematically recorded in iTMS
- User is assigned a default password which he needs to change immediately on first login
- The new password is known only to the end user.
- The user can change his own password as and when he wants to do so.
- In case the bank has implemented the biometric authentication process, user needs to also provide his finger scan at the time of login and also at the time of re-login on user lock

## Sample User Capability, Group and Type in CBS

| Description | Capability | Group | User Type |
|---|---|---|---|
| Clerk | 2 | 2 | 1 |
| Head Cashier | 2 | 2 | 60 |
| Special Assistant/ Officer | 7 | 5 | 40 |
| Vault Teller ( Branch Manager) | 9 | 5 | 50 |

| Description | Maker | Checker |
|---|---|---|
| Capability | 2 | 5, 7 , 9 |
| Capability | 5 | 7, 9 |
| Capability | 7 | 9 |



## Transaction Level Security

- User has the access to functions based on his user type, group and capability.
- There are various product level parameters set that ensure that a particular transaction is done only as expected by the bank
- There are various validations build in the system to restrict a wrong transaction happening.
- Facility of maker and checker is available for all transactions
- A transaction done by a user can be authorized only by a user having higher capability.
- An authorizer can view the transaction done by the maker during authorization and decide whether to authorize or reject a transaction

## Transaction Level Security

- There is a facility to correct a transaction that got inadvertently authorized by the checker.
- An authorizer can view the transaction done by the maker during authorization and decide whether to authorize or reject a transaction
- Authorizer can also put his remarks while rejecting a transaction that gets recorded in the system
- Various validations restrict the transactions from authorizing by giving exceptions to the end user in order to restrict the transactions that are against bank's policy e.g. cheque number does not pertain to account, the balance is going into negative in deposit account, balance crossing DP/Limit are few of the examples from many such other exceptions.



## Reports in CBS

- There are many reports generated in CBS at various frequencies that facilitate the end user to check both financial as well as non financial transactions executed in CBS
- The set of reports gives a capability to the bank to ensure that all transactions have been effected properly in the system and the system is in tallied state
- System also provides for monitoring reports that enable the branch/ bank to find out the irregular accounts/ transactions
- All these reports are generated automatically in CBS and also sent to branches and Bank HO through automated tool

## Reports in CBS - Contd

- Few examples of such reports are as under.
  - Teller wise cash reports
  - Supplementary Report
  - GL Comp Report
  - GL Control Report
  - Daily cash report
  - Branch and bank level trial balance, balance sheet, profit and loss
  - Branch level exception report
  - Irregularity related reports
  - Daily listing of all deposits and loan accounts
  - Transactions done by branches on accounts of non home branch
  - System generated transactions



## Reports in CBS - Contd

- Many reports and portals are provided to facilitate reconciliation of transactions happening through delivery channels
- The bank level users can use these on daily basis and reconcile their transactions promptly

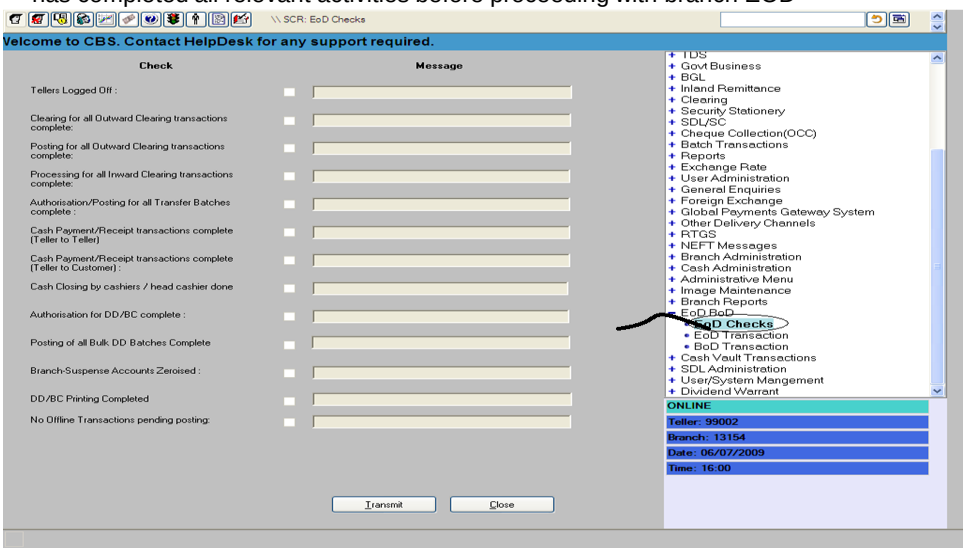
# ONLINE VVR

ONLINE-VVR---Knowledge-Document.pdf



## EOD checks

Various checks are performed during EOD process to ensure that branch has completed all relevant activities before proceeding with branch EOD



## Password protection by end users

Following suggestions should be strictly followed by end users in the bank.

- Do not share your password to others.
- Preferably keep a strong password.
- Do not use a password that can be easily guessed by others like own name, names of family members, vehicle number etc.
- Do not write your password, memorize it.
- Do not use others login id and password
- Change the password frequently
- Always lock your terminal while leaving the desk
- Do not allow anyone to shoulder surf while you are entering your password

Useful TIP

- Create a sentence/phrase that can be remembered well. Use its alphabets in specific order (e.g. first character of each word) with a combination of numbers and special characters
- Do not reveal the sentence or phrase to anyone

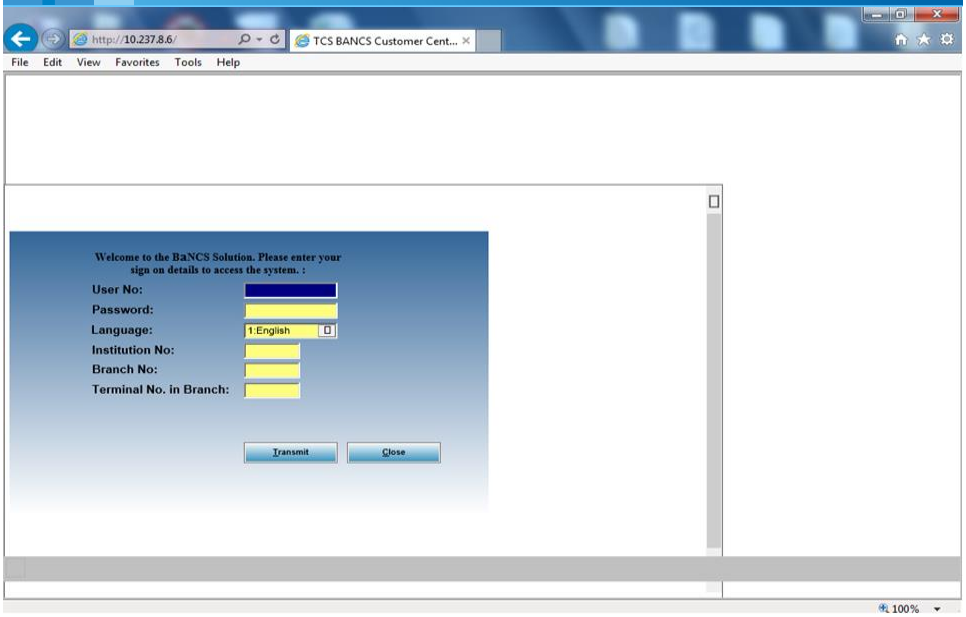


## Monitoring the bank

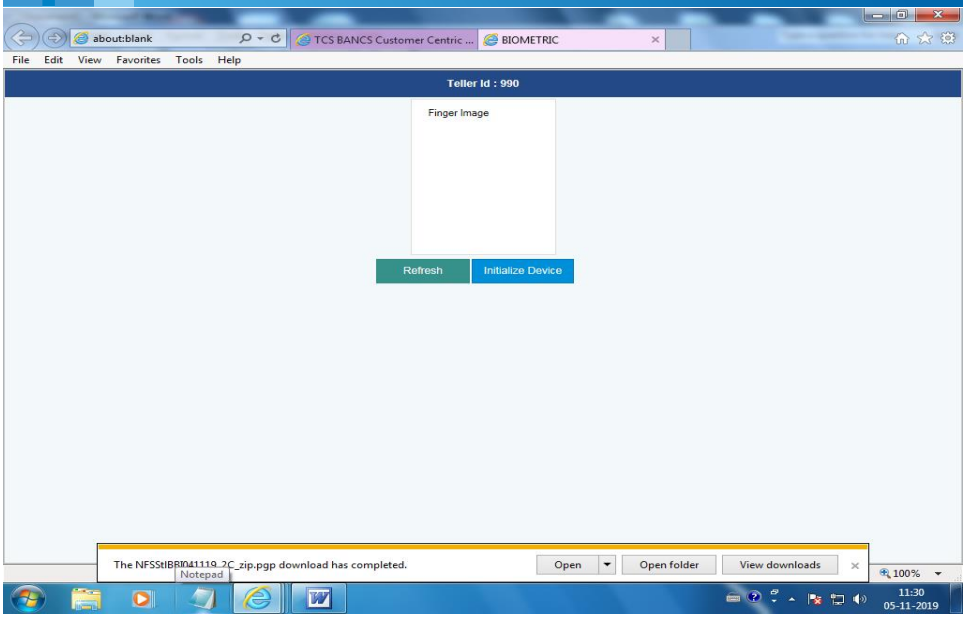
Following are few suggestions in order to protect the bank's interest. Best defense is to have good vigilance, strict processes and its implementation.

- Strictly follow Maker Checker process
- Have a monitoring cell dedicated to monitor CBS level activities of branches e.g.
  - User activity at branches
  - High value transactions in CBS and delivery channels
  - Ensure on time reconciliation of all transactions and channels
  - Regular visits to branches for inspection
  - Monitoring daily exception reports
  - Monitoring large variations in figures
  - Monitoring suspense accounts outstanding
  - Operations in dormant / inoperative accounts
  - Regular sample checking of branch transactions, non home transactions
- Have centralized processes wherever possible
- Implement biometric authentication if not yet done
- Sensitize bank level end users about security and being cautious while handing customer

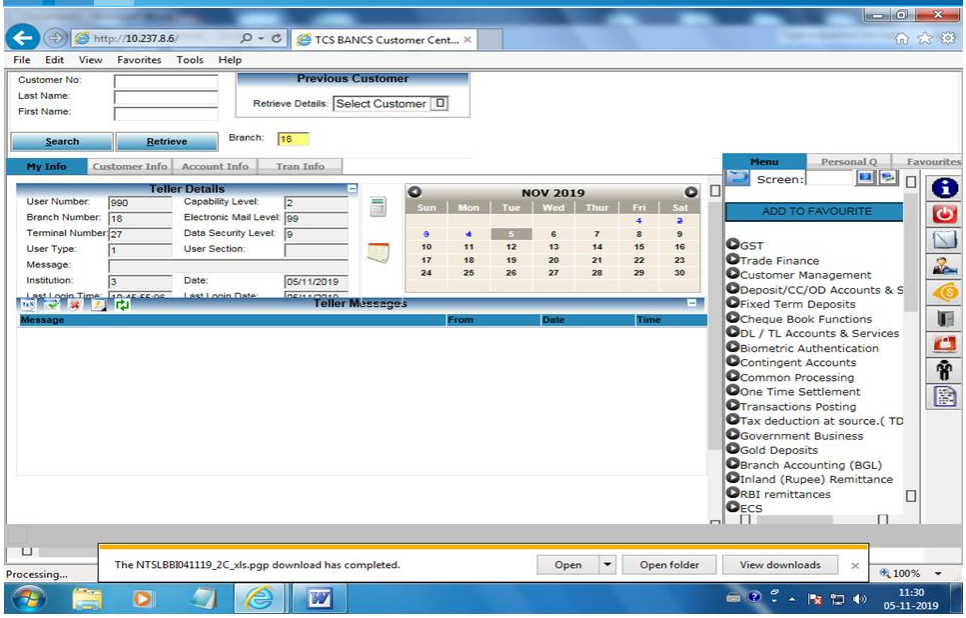
## User Login Screen



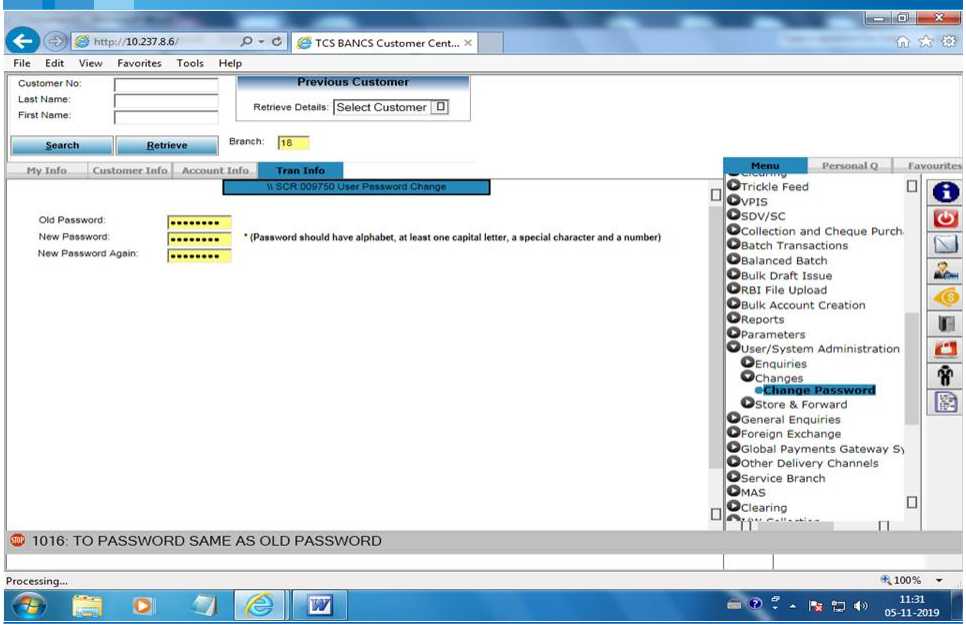

## Biometric Finger Scan during login



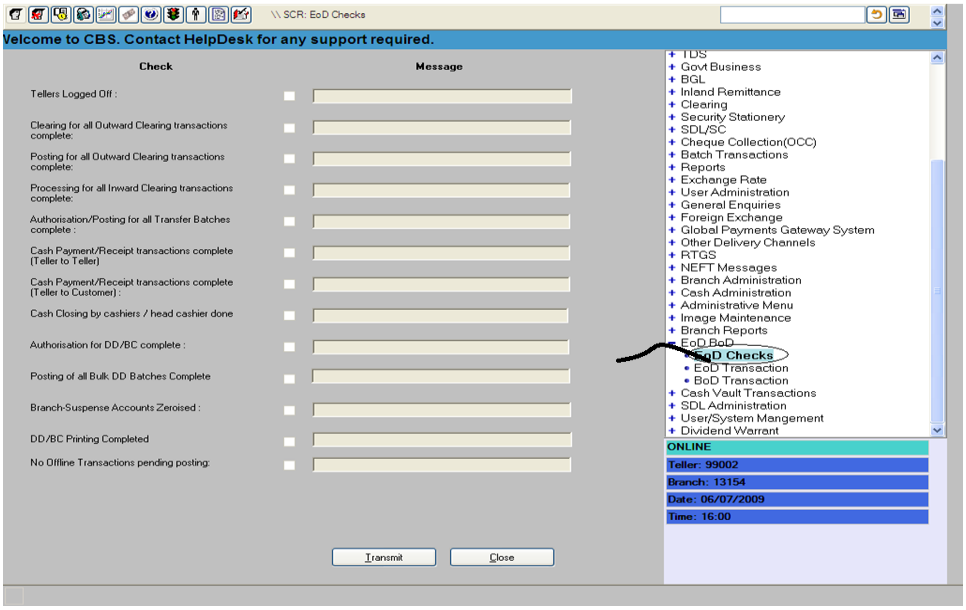
## Main Menu in CBS




## Password Change prompt in CBS on first login



## EOD checklist in CBS




# CBS Reports

## Daily CBS Reports

| Sr. No. | Report File | Report content | Report Frequency |
|---|---|---|---|
| 1 | GLCOM | GL Compare Report, which lists out the differences in balances between BGL and CGL | Daily |
| 2 | GLCNTR | GL Control Report, which lists out the balances in a some critical accounts those need to be monitored and zerolised on a daily basis. | Daily |
| 3 | BAL_IN_GL_ACC_GLCC_WISE_DET_ | customer & branch GL (BGL) accounts. It processes the branch originated transactions from BaNCS link as well as the Channel transactions. | Daily |
| 4 | GL-DayBook-gend0807 | GL Day Book, Reports giving GL wise daily Transactions | Daily |
| 5 | Trail Balance | Daily Trial Balance (Finance1) , Trial Balance in Liabilities and Assets format specially developed using Crystal Reports giving GL wise daily Receipts & Payments (i.e. net movement in a particular GL head) along with the Opening & Closing balance for a day for each GL head. | Daily |
| 6 | Voucher_varification_report_cfpd0331 | Voucher Verification Report for Customer accounts | Daily |
| 7 | EXCEPTION_REPORT_depd0670 | Shows the SUP-ID, SUP-ERR-NO, ERROR-DESCRIIPTION/ exceptional transaction | Daily |
| 8 | teller_report | Report that are available to the Head Office for their all transactions which have to branches on a daily basis before giving the EOD signal to the data centre. | Daily |
| 9 | CASH_REPORT-cfpd0903 | Cash Report, Vault teller needs to verify the reports for all tellers and accept the cash transferred to him by each of the teller. | Daily |
| 10 | Deposits_Balance_File_depd0586 | Daily account wise Deposits Balance report | Daily |
| 11 | LoansBalanceFile-lond2390 | Daily account wise Loans Balance Balance report | Daily |
| 12 | non_home_branch_cifd0363 | Transaction done from other branch / inter-bank fund transfer transactions (NEFT/ RTGS/ ECS etc.) | Daily |
| 13 | LOAN_IRREGULAR_REPORT | Loan repayment not proper ly done by customer | Daily |
| 14 | Listof_NPA_Accounts_lond2572 | NPA mark by branch (NPA Report) | Daily |



## Monthly CBS Reports

| Sr. No. | Report File | Report content | Report Frequency1 |
|---|---|---|---|
| 1 | CCOD_DEFAULTER_LIST | CCOD DEFAULTER accounts list | Monthly |
| 2 | Overdue_Notice_lond2384 | This Letter is a notification,runnng irregular/ overdue. You are, therefore, requested to regularize the position within 15 days from the date of this notice, failing which we shall be constrained to initiate appropriate action against you | Monthly |
| 3 | ACCOUNT_CLOSED_REPORT | Account closed in month at branch | Monthly |
| 4 | ACCOUNT_OPENED_REPORT | Account Opened in month at branch | Monthly |
| 5 | MONTHLY_TDS_DEDUCT | TDS deduct by system in month | Monthly |
| 6 | QUARTERLY_TDS_REPORT | TDS deduct by system list in a Quarter of month | Monthly |
| 7 | DD_PAID_OWN_BANK_REPORT | Demand Draft paid List | Monthly |
| 8 | Unpaid DD cfpm0342 | DD and PO Unpaid List | Monthly |
| 9 | Recovery_report | Recovery in Loan Accounts | Monthly |
| 10 | TDS_NOT_APPLIED_ACCOUNT_DETAILS_tdsn0101 | TDS not apply mark in CIF | Monthly |
| 11 | PREMATURE_TDR_CLOSURE.txt | PREMATURE TDR/STDR/RD CLOSURE REPORT | Monthly |

# Monthly upload Reports

1. CTR
2. CIBIL

## NEFT/RTGS Daily Reports

1. RECON - NEFT/RTGS Reconciliation
2. NEFT transaction Details
3. RTGS Transaction Details

## IMPS Daily Report

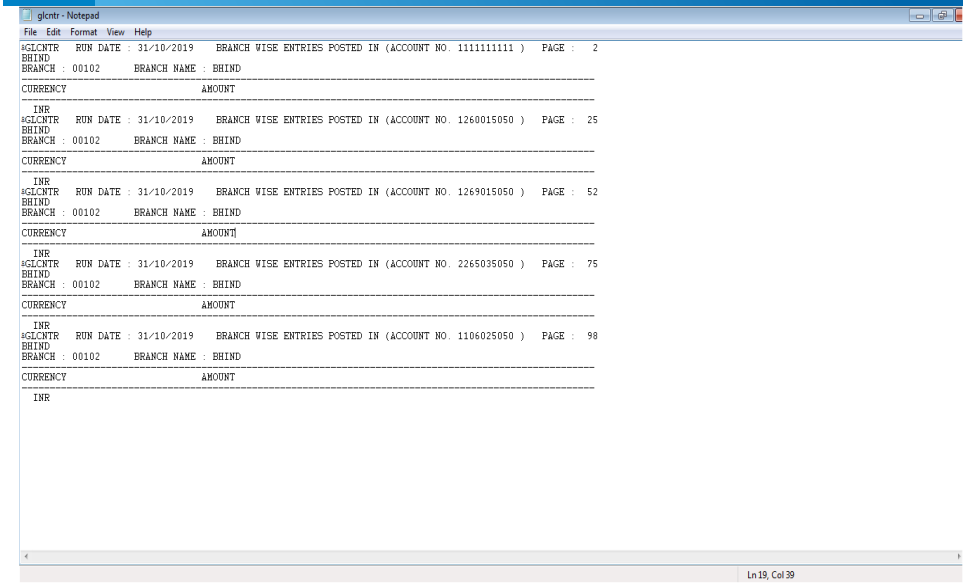
IMPS (IMPS Transaction Details)



# ATM Daily Report

| Sr. No. | Report File | Report content |
|---|---|---|
| 1 | BHGB_FAIL_ATM - | Failed Transaction of ATM Machine |
| 2 | BHGB_FAIL_BQR_ | Failed Transaction of Bharat QR code |
| 3 | BHGB_FAIL_ECO_ | Failed Transaction of E commerce (Online Transaction) |
| 4 | BHGB_FAIL_MATM_ | Failed Transaction of Micro ATM Transaction |
| 5 | BHGB_FAIL_POS_ | Failed Transaction of POS Machine Transaction |
| 6 | BHGB_SUCC_ATM_ | successful Transaction of ATM Machine |
| 7 | BHGB_SUCC_BQR_ | successful Transaction of Bharat QR code |
| 8 | BHGB_SUCC_ECO_ | successful Transaction of E commerce (Online Transaction) |
| 9 | BHGB_SUCC_MATM_ | successful Transaction of Micro ATM Transaction |
| 10 | BHGB_SUCC_POS_ | successful Transaction of POS Machine Transaction |

# Report Name glcntr.txt on Branch Server



glcntr - Notepad

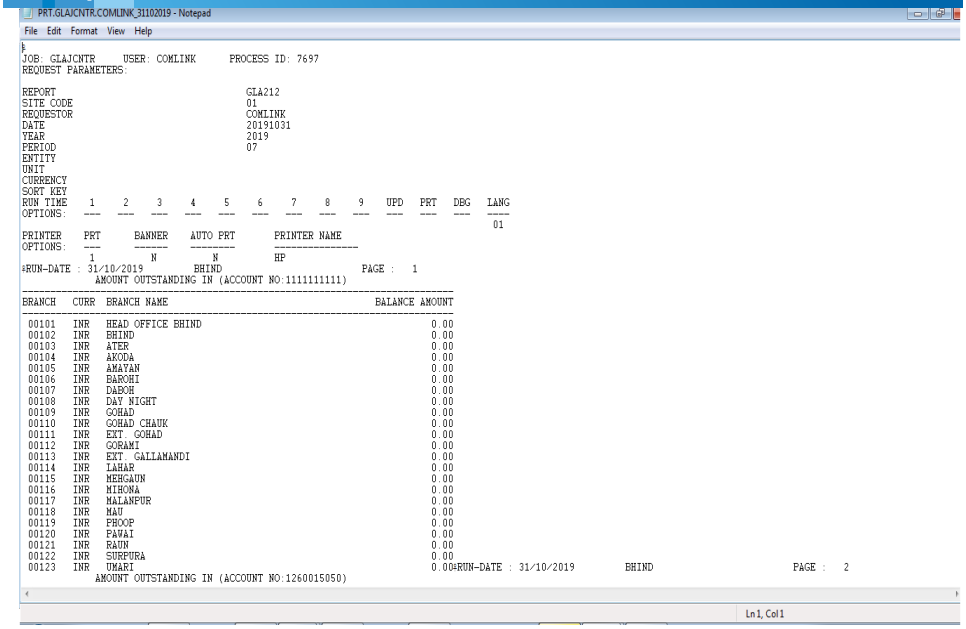
File Edit Format View Help

```
#GLCNTR   RUN DATE : 31/10/2019    BRANCH WISE ENTRIES POSTED IN (ACCOUNT NO. 1111111111 )   PAGE :   2
BHIND
BRANCH : 00102      BRANCH NAME : BHIND
-------------------------------------------------------------------------------------------------------------------
CURRENCY                          AMOUNT
-------------------------------------------------------------------------------------------------------------------
  INR
#GLCNTR   RUN DATE : 31/10/2019    BRANCH WISE ENTRIES POSTED IN (ACCOUNT NO. 1260015050 )   PAGE :   25
BHIND
BRANCH : 00102      BRANCH NAME : BHIND
-------------------------------------------------------------------------------------------------------------------
CURRENCY                          AMOUNT
-------------------------------------------------------------------------------------------------------------------
  INR
#GLCNTR   RUN DATE : 31/10/2019    BRANCH WISE ENTRIES POSTED IN (ACCOUNT NO. 1269015050 )   PAGE :   52
BHIND
BRANCH : 00102      BRANCH NAME : BHIND
-------------------------------------------------------------------------------------------------------------------
CURRENCY                          AMOUNT
-------------------------------------------------------------------------------------------------------------------
  INR
#GLCNTR   RUN DATE : 31/10/2019    BRANCH WISE ENTRIES POSTED IN (ACCOUNT NO. 2265035050 )   PAGE :   75
BHIND
BRANCH : 00102      BRANCH NAME : BHIND
-------------------------------------------------------------------------------------------------------------------
CURRENCY                          AMOUNT
-------------------------------------------------------------------------------------------------------------------
  INR
#GLCNTR   RUN DATE : 31/10/2019    BRANCH WISE ENTRIES POSTED IN (ACCOUNT NO. 1106025050 )   PAGE :   98
BHIND
BRANCH : 00102      BRANCH NAME : BHIND
-------------------------------------------------------------------------------------------------------------------
CURRENCY                          AMOUNT
-------------------------------------------------------------------------------------------------------------------
  INR
```

Ln 19, Col 39



# Report Name GLCNTR On HO Branch Server



PRT.GLAJCNTR.COMLINK_31102019 - Notepad

File Edit Format View Help

```
JOB: GLAJCNTR     USER: COMLINK      PROCESS ID: 7697
REQUEST PARAMETERS:

REPORT                                GLA212
SITE CODE                             01
REQUESTOR                             COMLINK
DATE                                  20191031
YEAR                                  2019
PERIOD                                07
ENTITY
UNIT
CURRENCY
SORT KEY
RUN TIME    1     2     3     4     5     6     7     8     9    UPD   PRT   DBG   LANG
OPTIONS:    ___   ___   ___   ___   ___   ___   ___   ___   ___  ___   ___   ___   _____
                                                                                    01

PRINTER    PRT      BANNER    AUTO PRT       PRINTER NAME
OPTIONS:   ___      ______    ________       ____________
             1          N          N          HP
#RUN-DATE : 31/10/2019          BHIND                PAGE :   1
          AMOUNT OUTSTANDING IN (ACCOUNT NO:1111111111)
-------------------------------------------------------------------------------------
BRANCH   CURR  BRANCH NAME                                        BALANCE AMOUNT
-------------------------------------------------------------------------------------
 00101   INR   HEAD OFFICE BHIND                                          0.00
 00102   INR   BHIND                                                      0.00
 00103   INR   ATER                                                       0.00
 00104   INR   AKODA                                                      0.00
 00105   INR   AMAYAN                                                     0.00
 00106   INR   BAROHI                                                    0.00
 00107   INR   DABOH                                                     0.00
 00108   INR   DAY NIGHT                                                 0.00
 00109   INR   GOHAD                                                     0.00
 00110   INR   GOHAD CHAUK                                               0.00
 00111   INR   EXT. GOHAD                                               0.00
 00112   INR   GORAMI                                                   0.00
 00113   INR   EXT. GALLAMANDI                                          0.00
 00114   INR   LAHAR                                                     0.00
 00115   INR   MEHGAUN                                                  0.00
 00116   INR   MIHONA                                                   0.00
 00117   INR   MALANPUR                                                 0.00
 00118   INR   MAU                                                       0.00
 00119   INR   PHOOP                                                     0.00
 00120   INR   PAWAI                                                     0.00
 00121   INR   RAUN                                                      0.00
 00122   INR   SURPURA                                                   0.00
 00123   INR   UMARI                                                     0.00#RUN-DATE : 31/10/2019          BHIND                PAGE :   2
          AMOUNT OUTSTANDING IN (ACCOUNT NO:1260015050)
```

Ln 1, Col 1

# Report Name glcom.txt

glcomp - Notepad

File Edit Format View Help

```
#GLCOMP    RUN DATE : 31/10/2019          EXCEPTION REPORT ON BANCS24 AND FINANCE-ONE ACCOUNTS                          PAGE :    2
BHIND
BRANCH : 00102       BRANCH NAME : BHIND
-------------------------------------------------------------------------------------------------------------------------------
BANCS24 ACCOUNTS                    BANCS24 AMOUNT  FINANCE-ONE ACCOUNTS            FINANCE-ONE AMOUNT       DIFFERENCE / ERROR
-------------------------------------------------------------------------------------------------------------------------------

00102INR2035010706              17,79,81,756.74- 00102INR2035010706              17,79,81,756.73-                      .01-
00102INR2035015003                5,81,13,163.33- 00102INR2035015003                5,81,13,163.32-                      .01-
00102INR2036010706                  19,11,616.00- 00102INR2036010706                  19,07,267.00-                 4,349.00-
```

Ln 10, Col 1

# Report Name GLGLCC

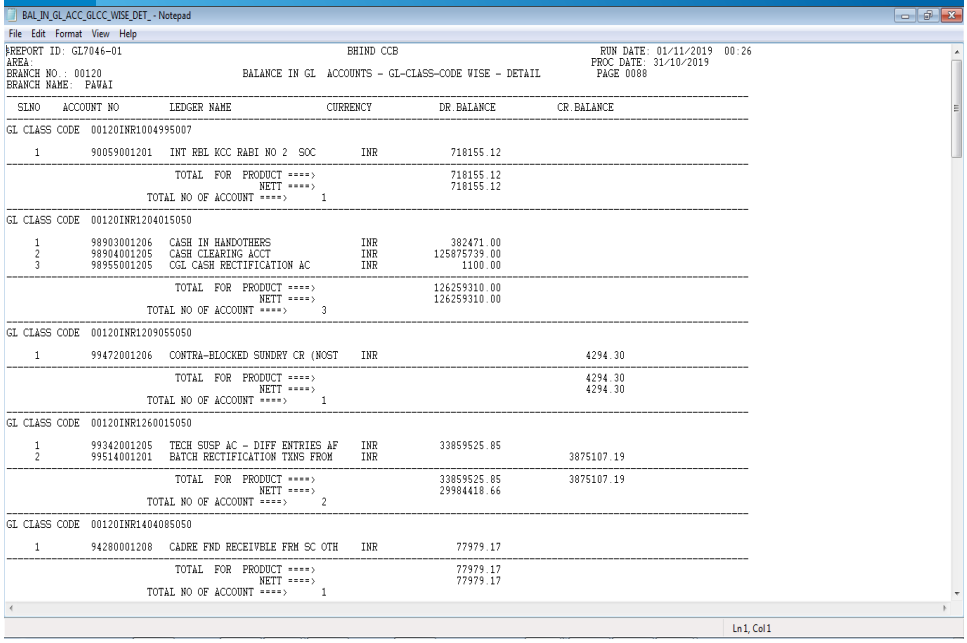
PRT.GLAJGLCC.COMLINK_31102019 - Notepad

File Edit Format View Help

```
#
JOB: GLAJGLCC     USER: COMLINK      PROCESS ID: 3029
REQUEST PARAMETERS:

REPORT                                GLA212
SITE CODE                             01
REQUESTOR                             COMLINK
DATE                                  20191031
YEAR                                  2019
PERIOD                                07
ENTITY
UNIT
CURRENCY
SORT KEY
RUN TIME    1    2    3    4    5    6    7    8    9   UPD  PRT  DBG  LANG
OPTIONS:   ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ----
                                                                        01

PRINTER    PRT      BANNER    AUTO PRT       PRINTER NAME
OPTIONS:   ---      ------    --------       ------------
            1          N         N          HP
                                            BHIND
#
RUN-DATE : 31/10/2019                EXCEPTION REPORT ON BANCS24 AND FINANCE-ONE ACCOUNTS                          PAGE :    1
-------------------------------------------------------------------------------------------------------------------------------
BANCS24 ACCOUNTS                    BANCS24 AMOUNT  FINANCE-ONE ACCOUNTS            FINANCE-ONE AMOUNT       DIFFERENCE / ERROR
-------------------------------------------------------------------------------------------------------------------------------

00101INR1401085050                    4,29,158.73   00101INR1401085050                    9,29,158.73             5,00,000.00-
00101INR1401105050                   33,85,076.72   00101INR1401105050                   28,85,076.72             5,00,000.00
00101INR1404155050                   19,74,934.32-  00101INR1404155050                                            19,74,934.32-
00101INR1511335050                4,02,67,817.42   00101INR1511335050                4,06,95,964.42             4,28,147.00-

                                                   00101INR2110015050                1,34,00,978.26  A/C MISSING IN BANCS24
                                                   00101INR2620055050               10,69,52,803.00-  A/C MISSING IN BANCS24

00102INR2035010706              17,79,81,756.74-  00102INR2035010706              17,79,81,756.73-                      .01-
00102INR2035015003                5,81,13,163.33-  00102INR2035015003                5,81,13,163.32-                      .01-

00102INR2036010706                  19,11,616.00-  00102INR2036010706                  19,07,267.00-                 4,349.00-
00103INR1404155050                  10,86,775.30-  00103INR1404155050                                            10,86,775.30-
00103INR1968995012                   1,06,954.98-                                                          A/C MISSING IN FIN-ONE
00103INR1971995012                      12,641.86-  00103INR1971995012                      12,641.86             25,283.72-

                                                   00103INR2249015012                    6,21,231.00-  A/C MISSING IN BANCS24

00104INR1004015012                2,01,55,312.81   00104INR1004015012                2,01,55,312.82                      .01-

00104INR1034015012                   1,85,046.00   00104INR1034015012                   1,36,475.00             48,571.00
00104INR1034995012                     14,418.36                                                           A/C MISSING IN FIN-ONE#
RUN-DATE : 31/10/2019                EXCEPTION REPORT ON BANCS24 AND FINANCE-ONE ACCOUNTS                          PAGE :    3
```

Ln 39, Col 1

# Report Name BAL_IN_GL_ACC_GLCC_WISE_DET_.txt



BAL_IN_GL_ACC_GLCC_WISE_DET_ - Notepad

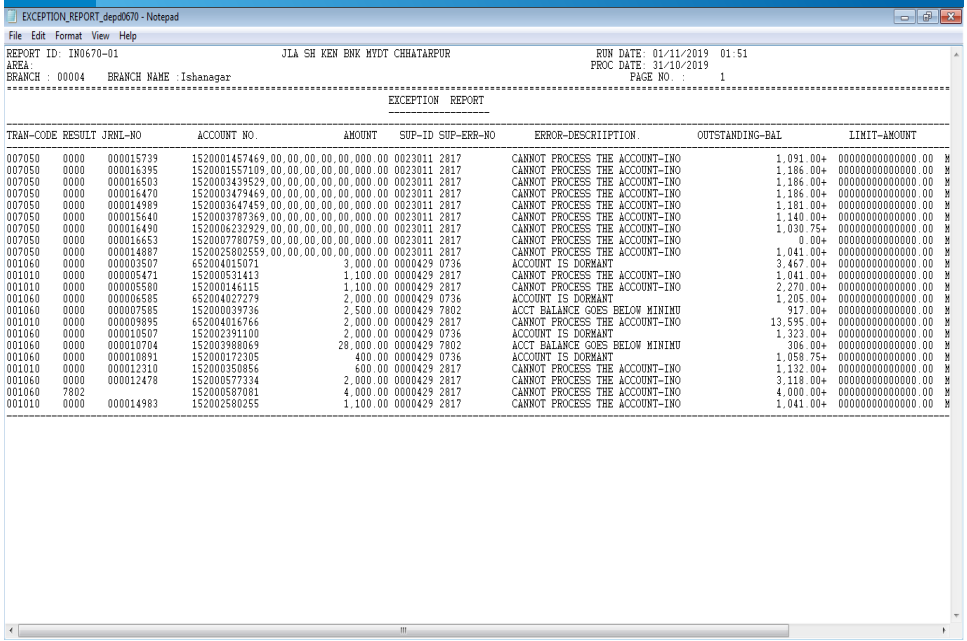
File Edit Format View Help

```
REPORT ID: GL7046-01                                  BHIND CCB                                  RUN DATE: 01/11/2019  00:26
AREA:                                                                                            PROC DATE: 31/10/2019
BRANCH NO. : 00120                    BALANCE IN GL  ACCOUNTS - GL-CLASS-CODE WISE - DETAIL      PAGE 0088
BRANCH NAME:  PAWAI
```

| SLNO | ACCOUNT NO | LEDGER NAME | CURRENCY | DR.BALANCE | CR.BALANCE |
|---|---|---|---|---|---|
| GL CLASS CODE | 00120INR1004995007 | | | | |
| 1 | 90059001201 | INT RBL KCC RABI NO 2 SOC | INR | 718155.12 | |
| | | TOTAL FOR PRODUCT ====> | | 718155.12 | |
| | | NETT ====> | | 718155.12 | |
| | | TOTAL NO OF ACCOUNT ====> 1 | | | |
| GL CLASS CODE | 00120INR1204015050 | | | | |
| 1 | 98903001206 | CASH IN HANDOTHERS | INR | 382471.00 | |
| 2 | 98904001205 | CASH CLEARING ACCT | INR | 125875739.00 | |
| 3 | 98955001205 | CGL CASH RECTIFICATION AC | INR | 1100.00 | |
| | | TOTAL FOR PRODUCT ====> | | 126259310.00 | |
| | | NETT ====> | | 126259310.00 | |
| | | TOTAL NO OF ACCOUNT ====> 3 | | | |
| GL CLASS CODE | 00120INR1209055050 | | | | |
| 1 | 99472001206 | CONTRA-BLOCKED SUNDRY CR (NOST | INR | | 4294.30 |
| | | TOTAL FOR PRODUCT ====> | | | 4294.30 |
| | | NETT ====> | | | 4294.30 |
| | | TOTAL NO OF ACCOUNT ====> 1 | | | |
| GL CLASS CODE | 00120INR1260015050 | | | | |
| 1 | 99342001205 | TECH SUSP AC - DIFF ENTRIES AF | INR | 33859525.85 | |
| 2 | 99514001201 | BATCH RECTIFICATION TXNS FROM | INR | | 3875107.19 |
| | | TOTAL FOR PRODUCT ====> | | 33859525.85 | 3875107.19 |
| | | NETT ====> | | 29984418.66 | |
| | | TOTAL NO OF ACCOUNT ====> 2 | | | |
| GL CLASS CODE | 00120INR1404085050 | | | | |
| 1 | 94280001208 | CADRE FND RECEIVBLE FRM SC OTH | INR | 77979.17 | |
| | | TOTAL FOR PRODUCT ====> | | 77979.17 | |
| | | NETT ====> | | 77979.17 | |
| | | TOTAL NO OF ACCOUNT ====> 1 | | | |

Ln 1, Col 1

# Report Name EXCEPTION_REPORT_depd0670



EXCEPTION_REPORT_depd0670 - Notepad

File Edit Format View Help

```
REPORT ID: IN0670-01                          JLA SH KEN BNK MYDT CHHATARPUR                  RUN DATE: 01/11/2019  01:51
AREA:                                                                                         PROC DATE: 31/10/2019
BRANCH : 00004    BRANCH NAME :Ishanagar                                                      PAGE NO. :     1
```

EXCEPTION REPORT

| TRAN-CODE | RESULT | JRNL-NO | ACCOUNT NO. | AMOUNT | SUP-ID | SUP-ERR-NO | ERROR-DESCRIIPTION. | OUTSTANDING-BAL | LIMIT-AMOUNT | |
|---|---|---|---|---|---|---|---|---|---|---|
| 007050 | 0000 | 000015739 | 1520001457469.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 1,091.00+ | 00000000000000.00 | M |
| 007050 | 0000 | 000016395 | 1520001557109.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 1,186.00+ | 00000000000000.00 | M |
| 007050 | 0000 | 000016503 | 1520003439529.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 1,186.00+ | 00000000000000.00 | M |
| 007050 | 0000 | 000016470 | 1520003479469.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 1,186.00+ | 00000000000000.00 | M |
| 007050 | 0000 | 000014989 | 1520003647459.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 1,181.00+ | 00000000000000.00 | M |
| 007050 | 0000 | 000015440 | 1520003787369.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 1,140.00+ | 00000000000000.00 | M |
| 007050 | 0000 | 000016490 | 1520006232929.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 1,030.75+ | 00000000000000.00 | M |
| 007050 | 0000 | 000016653 | 1520007780759.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 0.00+ | 00000000000000.00 | M |
| 007050 | 0000 | 000014887 | 1520025802559.00.00.00.00.00.000.00 | 0023011 | 2817 | | CANNOT PROCESS THE ACCOUNT-INO | 1,041.00+ | 00000000000000.00 | M |
| 001060 | 0000 | 000003507 | 652004015071 | 3,000.00 | 0000429 | 0736 | ACCOUNT IS DORMANT | 3,467.00+ | 00000000000000.00 | M |
| 001010 | 0000 | 000005471 | 152000531413 | 1,100.00 | 0000429 | 2817 | CANNOT PROCESS THE ACCOUNT-INO | 1,041.00+ | 00000000000000.00 | M |
| 001010 | 0000 | 000005580 | 152000146115 | 1,100.00 | 0000429 | 2817 | CANNOT PROCESS THE ACCOUNT-INO | 2,270.00+ | 00000000000000.00 | M |
| 001060 | 0000 | 000006585 | 652004027279 | 2,000.00 | 0000429 | 0736 | ACCOUNT IS DORMANT | 1,205.00+ | 00000000000000.00 | M |
| 001060 | 0000 | 000007585 | 152000039736 | 2,500.00 | 0000429 | 7802 | ACCT BALANCE GOES BELOW MINIMU | 917.00+ | 00000000000000.00 | M |
| 001010 | 0000 | 000009895 | 652004016766 | 2,000.00 | 0000429 | 2817 | CANNOT PROCESS THE ACCOUNT-INO | 13,595.00+ | 00000000000000.00 | M |
| 001060 | 0000 | 000010507 | 152002391100 | 2,000.00 | 0000429 | 0736 | ACCOUNT IS DORMANT | 1,323.00+ | 00000000000000.00 | M |
| 001060 | 0000 | 000010704 | 152003988069 | 28,000.00 | 0000429 | 7802 | ACCT BALANCE GOES BELOW MINIMU | 306.00+ | 00000000000000.00 | M |
| 001060 | 0000 | 000010891 | 152000172305 | 400.00 | 0000429 | 0736 | ACCOUNT IS DORMANT | 1,058.75+ | 00000000000000.00 | M |
| 001010 | 0000 | 000012310 | 152000350856 | 600.00 | 0000429 | 2817 | CANNOT PROCESS THE ACCOUNT-INO | 1,132.00+ | 00000000000000.00 | M |
| 001060 | 0000 | 000012478 | 152000577334 | 2,000.00 | 0000429 | 2817 | CANNOT PROCESS THE ACCOUNT-INO | 3,118.00+ | 00000000000000.00 | M |
| 001060 | 7802 | | 152000587081 | 4,000.00 | 0000429 | 2817 | CANNOT PROCESS THE ACCOUNT-INO | 4,000.00+ | 00000000000000.00 | M |
| 001010 | 0000 | 000014983 | 152002580255 | 1,100.00 | 0000429 | 2817 | CANNOT PROCESS THE ACCOUNT-INO | 1,041.00+ | 00000000000000.00 | M |

# Report Name non_home_branch_cifd0363

non_home_branch_cifd0363 - Notepad

File Edit Format View Help

REPORT ID: SY0363-01 JLA SH KEN BNK MYDT CHHATARPUR RUN DATE: 01/11/2019 01:49
AREA: PROC DATE: 31/10/2019-ID
BRANCH NO : 4 BRANCH NAME : Ishanagar

| SR.NO | OTHER-BRANCH-CODE | CUSTOMER NAME | ACCOUNT NUMBER | PRODUCT NAME | TXN-CODE | TXN-DEBIT- |
|---|---|---|---|---|---|---|
| 1 | 22 | Mr. LAKHAN SINGH | 152000252599 | SBCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 2 | 22 | Mr. LAXMEE PARSAD TIWARI | 152000281042 | SBCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 3 | 22 | Mr. JAMNA PRASAD TIWARI | 152000296648 | SBCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 4 | 22 | Mr. MADAN PRASAD PATEL S/O BINDABAN PATEL | 152000504354 | SBCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 5 | 22 | Mrs. VIMLA AHIRWAR | 152000669861 | SBNCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 6 | 22 | Mrs. HEERA BAI AHIRWAR W/O BABOO LAL AHIRWAR | 152000773178 | SBNCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 7 | 22 | Mrs. MOANI RAJA W/O VEERENDRA SINGH | 152003267795 | SBNCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 8 | 22 | Mr. RAMESH CHANDRA RAWAT S/O CHURAMAN RAWAT | 152003431020 | SBCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 9 | 22 | Mrs. LEELA BATI SEN W/O SHANKAR SEN | 652004010980 | SBNCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 10 | 22 | SHIVAM SVA- SAHAYATA SAMUH BIHTHA | 652004047387 | SBCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 11 | 99922 | Mrs. BITTAN KACHI W/O RAM LAL KACHI | 152002620755 | SBNCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 12 | 99922 | Mr. HARDAYAL AHIRWAR S/O TIJBA AHIRWAR | 652004011225 | SBNCHQ-IND | 1045 | |
| | | | | | TOTAL: | |
| 13 | 99922 | Mr. BHOLA AHIRWAR S/O GANESHA AHIRWAR | 652004040336 | SBNCHQ-NO FRILLS | 1045 | |
| | | | | | TOTAL: | |
| | | | | | BRANCH TOTAL: | |

Ln1 Col1

# Teller Report ,on HO Branch Server All Transaction doing branch level

EditPlus - [Z:\CDC\REPORTS\DHAR_DCCB\20191031\teller_report.prt]

File Edit View Search Document Project Tools Browser Zen Coding Window Help

20191031|11:29:26|00020|0000514|007050|000005605|CHANGE DETAILS PROMPT SCREEN |00000155007435121|

--- TELLER REPORT ---

Page No:- 27

| LOG DATE | TIME | BR NO | TELLER | TRN NO | JRN NO | DISCRIPTION | ACCOUNT NO | MAKER | CHECKER |
|---|---|---|---|---|---|---|---|---|---|
| 20191031 | 11:29:27 | 00025 | 0000521 | 069029 | 000005606 | PREFETCH TRANSACTION | 00000655025002327 | | |
| 20191031 | 11:29:27 | 00023 | 0001001 | 069029 | 000005607 | PREFETCH TRANSACTION | 00000155000679118 | | |
| 20191031 | 11:29:30 | 00007 | 0001011 | 069029 | 000005608 | PREFETCH TRANSACTION | 00000655007027547 | | |
| 20191031 | 11:29:30 | 00003 | 0001007 | 069029 | 000005609 | PREFETCH TRANSACTION | 00000655003021877 | | |
| 20191031 | 11:29:32 | 00016 | 0000647 | 069029 | 000005610 | PREFETCH TRANSACTION | 00000155000917531 | | |
| 20191031 | 11:29:33 | 00017 | 0000836 | 001060 | 000005611 | CASH WITHDRAWAL | 00000655017019874 | 0000836 | 0000657 |
| 20191031 | 11:29:34 | 00024 | 0000979 | 001060 | 000005612 | CASH WITHDRAWAL | 00000155000706788 | 0000979 | 0000662 |
| 20191031 | 11:29:36 | 00021 | 0000992 | 069029 | 000005613 | PREFETCH TRANSACTION | 00000655021008425 | | |
| 20191031 | 11:29:36 | 00007 | 0000587 | 069029 | 000005614 | PREFETCH TRANSACTION | 00000155006857701 | | |
| 20191031 | 11:29:37 | 00099 | 0001017 | 069029 | 000005615 | PREFETCH TRANSACTION | 00000093065000991 | | |
| 20191031 | 11:29:38 | 00009 | 0000981 | 069029 | 000005616 | PREFETCH TRANSACTION | 00000155000423825 | | |
| 20191031 | 11:29:38 | 00025 | 0000521 | 001060 | 000005617 | CASH WITHDRAWAL | 00000155000003978 | 0000521 | 0000724 |
| 20191031 | 11:29:40 | 00014 | 0001012 | 069029 | 000005618 | PREFETCH TRANSACTION | 00000155000829484 | | |
| 20191031 | 11:29:40 | 00019 | 0000962 | 000600 | 000005619 | UPDATE PASSBOOK | 00000155000185244 | | |
| 20191031 | 11:29:41 | 00101 | 0000915 | 009755 | 000005620 | TELLER FORCED CLOSURE | 100009909YR0RbdI 23 | | |
| 20191031 | 11:29:41 | 00026 | 0000872 | 069029 | 000005621 | PREFETCH TRANSACTION | 00000155000711405 | | |
| 20191031 | 11:29:42 | 00101 | 0000915 | 001010 | 000005622 | CASH DEPOSIT | 00000655101020861 | 0000915 | 0000658 |
| 20191031 | 11:29:43 | 00006 | 0000737 | 000600 | 000005623 | UPDATE PASSBOOK | 00000155000488170 | | |
| 20191031 | 11:29:45 | 00015 | 0001002 | 069029 | 000005624 | PREFETCH TRANSACTION | 00000155007421902 | | |
| 20191031 | 11:29:46 | 00019 | 0000962 | 000602 | 000005625 | PASSBOOK LINE NO UPDATE | 00000155000185244 | | |
| 20191031 | 11:29:46 | 00007 | 0000973 | 001010 | 000005626 | CASH DEPOSIT | 00000155006857701 | 0000973 | 0000587 |
| 20191031 | 11:29:46 | 00006 | 0000737 | 000602 | 000005627 | PASSBOOK LINE NO UPDATE | 00000155000488170 | | |
| 20191031 | 11:29:47 | 00008 | 0001004 | 069029 | 000005628 | PREFETCH TRANSACTION | 00000155000093293 | | |
| 20191031 | 11:29:48 | 00003 | 0001007 | 000600 | 000005629 | UPDATE PASSBOOK | 00000655003021877 | | |
| 20191031 | 11:29:49 | 00003 | 0001007 | 000602 | 000005630 | PASSBOOK LINE NO UPDATE | 00000655003021877 | | |
| 20191031 | 11:29:49 | 00018 | 0000545 | 069029 | 000005631 | PREFETCH TRANSACTION | 00000155005583603 | | |
| 20191031 | 11:29:49 | 00027 | 0001016 | 069029 | 000005632 | PREFETCH TRANSACTION | 00000155000681718 | | |
| 20191031 | 11:29:50 | 00016 | 0000925 | 001060 | 000005633 | CASH WITHDRAWAL | 00000155000917531 | 0000925 | 0000647 |
| 20191031 | 11:29:50 | 00101 | 0000990 | 009001 | 000005634 | OPEN TELLER | * | | |
| 20191031 | 11:29:52 | 00201 | 0000654 | 069029 | 000005635 | PREFETCH TRANSACTION | 00000655201023143 | | |
| 20191031 | 11:29:53 | 00020 | 0000864 | 001060 | 000005636 | CASH WITHDRAWAL | 00000655020021048 | | |
| 20191031 | 11:29:54 | 00015 | 0000571 | 069029 | 000005637 | PREFETCH TRANSACTION | 00000655015013091 | | |
| 20191031 | 11:29:55 | 00101 | 0000915 | 009755 | 000005638 | TELLER FORCED CLOSURE | 100009909YR0RbdI 23 | | |
| 20191031 | 11:30:01 | 00201 | 0000993 | 000600 | 000005639 | UPDATE PASSBOOK | 00000655201029600 | | |
| 20191031 | 11:30:02 | 00025 | 0000724 | 069029 | 000005640 | PREFETCH TRANSACTION | 00000655025002327 | | |

teller_report.prt

For Help, press F1 ln 1 col 1 15824 0C UNIX ANSI

# अधिसूचनाएं

**बैंकों में साइबर सिक्यूरिटी की रूपरेखा**

**आरबीआई/2015-16/418**
**डीबीएस.सीओ.सीएसआईटीई.बीसी 11/33.01.001/2015-16**

**ज्येष्ठ १२, १९३८ (शक)**
**02 जून, 2016**

अध्यक्ष / प्रबंध निदेशक / मुख्य कार्यपालक अधिकारी
समस्त अनुसूचित वाणिज्यिक बैंक (क्षेत्रीय ग्रामीण बैंकों को छोडकर)

महोदया / महोदय

**बैंकों में साइबर सिक्यूरिटी की रूपरेखा**

**प्रस्तावना**

बैंकों और उनके संघटकों द्वारा सूचना प्रौद्योगिकी का प्रयोग तेजी से बढ़ा है और यह अब बैंकों की परिचालनीय कार्यनीति का एक महत्वपूर्ण अंग है। भारतीय रिज़र्व बैंक ने दिनांक 29 अप्रैल, 2011 के परिपत्र डीबीएस.सीओ.आईटीसी.बीसी.सं.6/31.02.008/2010-11 के माध्यम से इन्फोर्मेशन सिक्यूरिटी, इलेक्ट्रोनिक बैंकिंग, तकनीकी जोखिम प्रबंधन और साइबर धोखाधड़ी (जी. गोपाल कृष्ण समिति) के संबंध में दिशानिर्देश जारी किए थे जिसमें यह बताया गया था कि कार्यान्वयन हेतु बताए गए उपाय स्थायी नहीं है और बैंक नए संवर्धन विकास और उत्पन्न कठिनाइयों के आधार पर अपनी नीतियों, प्रणालियों और तकनीकों को सक्रिय रूप से तैयार करे / ठीक करें और संशोधित करते रहें ।

2. तब से, बैंकों द्वारा तकनीक के प्रयोग में और अधिक बढ़ोतरी हुई है। दूसरी ओर, गत समय में साइबर घटनाओं/आक्रमणों की संख्या, अंतराल और प्रभाव में काफी वृद्धि हुई है, विशेष रूप से बैंक सहित वित्तीय क्षेत्र के मामले, जो संकेत दे रहे हैं कि बैंकों में सुदृढ़ साइबर सिक्यूरिटी / आघात-सहनीयता की रूपरेखा को लागू करने की तत्काल आवश्यकता है और नियमित आधार पर बैंकों में पर्याप्त साइबर-सिक्यूरिटी की तैयारी सुनिश्चित करना आवश्यक है। आसान होते साइबर खतरे, इनका विकासरत स्वरूप, स्तर/वेग में वृद्धि, उत्प्रेरणा और बैंकिंग प्रणाली में साइबर-खतरों की उपस्थिती को ध्यान में रखते हुए, यह आवश्यक है कि साइबर जोखिमों से निपटने के लिए वर्तमान सुरक्षा में सुधार द्वारा बैंकिंग प्रणाली की आघात-सहनीयता में सुधार किया जाए । प्रतिकूल घटनाओं / बाधाओं, जब कभी घटित हों, से निपटने में अनुकूलनीय घटना प्रतिक्रिया, प्रबंध एवं पुनःप्राप्ति रूपरेखा शामिल होंगे, लेकिन ये यही तक सीमित नहीं होंगे।

**बोर्ड द्वारा अनुमोदित साइबर सिक्यूरिटी नीति की आवश्यकता**

3. बैंकों को अपने बोर्ड द्वारा विधिवत अनुमोदित साइबर सिक्यूरिटी नीति को तत्काल लागू करना चाहिए जिसमें साइबर खतरों से लड़ने के लिए उचित उपायों की रणनीति तथा कारोबार की जटिलताओं का स्तर और जोखिम का स्वीकार्य स्तर स्पष्ट होने चाहिए। इस संबंध में पुष्टि जल्द से जल्द साइबर सुरक्षा और सूचना प्रौद्योगिकी जांच कक्ष (सीएसआईटीई), बैंकिंग पर्यवेक्षण विभाग, भारतीय रिज़र्व बैंक, केंद्रीय कार्यालय, वर्ल्ड ट्रेड सेंटर-1, चौथी मंजिल, कफ परेड, मुंबई-400005 को की जाए, जो की किसी भी स्थिति में 30 सितंबर, 2016 के बाद नहीं हो।

यह सुनिश्चित किया जाए कि कार्यनीति में निम्नलिखित महत्वपूर्ण पहलू शामिल हों:

**साइबर सिक्यूरिटी नीति, बैंक की विस्तृत आईटी नीति / आईएस सिक्यूरिटी नीति से भिन्न हो**

4. साइबर सुरक्षित माहौल में सम्पूर्ण बैंक के योगदान की आवश्यकताओं पर ध्यान देने हेतु साइबर सिक्यूरिटी नीति, विस्तृत आईटी नीति / आईएस सिक्यूरिटी नीति से भिन्न एवं अलग होनी चाहिए ताकि यह साइबर खतरों के जोखिमों और इन जोखिमों से निपटने / कम करने के उपायों पर प्रकाश डाल सके।

5. आकार, प्रणाली, तकनीकी कठिनाइयाँ, डिजिटल उत्पाद, हितधारक और खतरों की संभावना बैंकवार बदलती रहती है और अतः यह महत्वपूर्ण है कि अंतर्निहित जोखिमों की पहचान की जाए और उचित साइबर सिक्यूरिटी रूपरेखा को अपनाने के लिए नियंत्रण स्थापित किया जाए। जबकि अंतर्निहित जाखिमों की पहचान तथा मूल्यांकन करने के लिए, बैंकों से अपेक्षित है कि वे अपनाए गए तकनीकों, कारोबार और विनियमित आवश्यकताओं का सामंजस्य, स्थापित कनैक्शन, आपूर्ति चैनल, ऑनलाइन/मोबाइल प्रोडक्ट, तकनीकी सेवाएं, संगठनात्मक परिवेश और आंतरिक तथा बाह्य खतरों की गणना करें। अंतर्निहित जोखिमों के स्तर के आधार पर बैंकों से अपेक्षित है कि वे अपने जोखिमों को निम्न, सामान्य, उच्च, अति उच्च के रूप में पहचान करें अथवा इस प्रकार के कोई अन्य वर्गीकरण को अपनाएं। अंतर्निहित जोखिमों के मूल्यांकन करते समय कारोबार घटकों के जोखिमों को भी ध्यान में रखा जाए। नियंत्रणों के मूल्यांकन के समय, बोर्ड की ज़िम्मेदारी, नीतियां, प्रक्रिया, साइबर जोखिम प्रबंधन आर्किटेक्चर सहित अनुभवी और योग्य स्रोत, प्रशिक्षण एवं परिवेश, खतरा आसूचना को इकठ्ठा करने की व्यवस्था, बैंकों से प्राप्त खतरा आसूचना की स्थितियों की तुलना में प्राप्त स्थितियों की निगरानी एवं विश्लेषण, सूचना आदान-प्रदान करने की व्यवस्था (सहयोगी बैंकों के बीच, आईडीआरबीटी/आरबीआई/सीईआरटी-इन के साथ), सुरक्षात्मक, खुफिया और सुधारात्मक साइबर सिक्यूरिटी नियंत्रण, वेंडर प्रबंधन, घटना प्रबंधन तथा प्रतिक्रिया को दर्शाया जाए।

**नियमित चौकसी की व्यवस्था**

6. समय के उचित अंतराल पर संवेदनशीलताओं की जांच करना बहुत ही महत्वपूर्ण है। साइबर-आक्रमण का स्वरूप इस प्रकार है कि वे कभी भी घटित हो सकते हैं और अनुमान से परे भी हो सकते हैं। अतः, यह आदेश दिया जाता है कि एसओसी (सिक्यूरिटी ऑपरेशन सेंटर) यथाशीघ्र स्थापित किया जाए, यदि ऐसा पहले नहीं किया गया हो । यह भी आवश्यक है कि यह केंद्र नियमित चौकसी को सुनिश्चित करे तथा आने वाले साइबर खतरों के हाल ही के स्वरूपों को नियमित आधार पर अद्यतन करे।

**आईटी आर्किटेक्चर सुरक्षा के लिए हितकर हो**

7. आईटी आर्किटेचर इस तरह से बनाया जाए कि वह सदैव लागू किए जाने वाले सुरक्षा उपायों की सुविधा का ध्यान रखे। बोर्ड की आईटी उप समिति द्वारा इसकी समीक्षा की जाए और यदि आवश्यक हो तो, इसके जोखिम मूल्यांकन के अनुसार इसे चरणबद्ध तरीके से अद्यतन किया जाए । बैंक द्वारा लिए जाने वाले जोखिम तथा लागत/संभाव्य लागत ट्रेड-ऑफ से संबन्धित निर्णय लिखित में दर्ज किए जाए ताकि बाद में उनका उचित पर्यवेक्षी मूल्यांकन किया जा सके।

8. अनुबंध 1 में दिए गए न्यूनतम मूलभूत साइबर सुरक्षा तथा रेसिलियन्स फ्रेमवर्क बैंकों द्वारा कार्यान्वित किए जाएंगे जो उदाहरणार्थ हैं, सम्पूर्ण नहीं। बैंकों को एक सिक्यूरिटी ऑपरेशन सेंटर (एसओसी) को स्थापित करने तथा उसे प्रारम्भ करने की प्रक्रिया को पूरी सक्रियता के साथ शुरू करना होगा ताकि रियल टाइम में साइबर जोखिमों की निगरानी तथा प्रबंधन किया जा सके। एसओसी का एक निर्देशात्मक कान्फ़िगरेशन अनुबंध 2 में दिया गया है ।

**व्यापक रूप से नेटवर्क तथा डाटाबेस सुरक्षा पर गौर करना**

9. हाल ही की घटनाओं के कारण प्रत्येक बैंक में नेटवर्क सुरक्षा की बेहतर तरीके से समीक्षा करने की आवश्यकता पर ध्यान केंद्रित हुआ है। इसके अतिरिक्त, यह पाया गया है कि कुछ व्यावसायिक या परिचालनीय अपेक्षाओं को पूरी करने के मद्देनजर एक विशिष्ट समयावधि के लिए नेटवर्क/डाटाबेस में कई बार कनैक्शन की अनुमति दी जाती है। हालांकि, जिसे चूकवश बंद नहीं किया जाता है जिसके फलस्वरूप नेटवर्क/डाटाबेस साइबर-हमलों की चपेट में आ सकता है। यह आवश्यक है कि नेटवर्कों तथा डाटाबेसो में अप्राधिकृत रूप से एक्सस करने की अनुमति नहीं दी जानी चाहिए तथा जब कभी अनुमति दी जाए, तो निर्धारित प्रक्रियाओं का अनिवार्य रूप से पालन किया जाए। इस प्रकार के नेटवर्कों तथा डाटाबेसों की जिम्मेवारी स्पष्ट रूप से दर्शायी जानी चाहिए तथा अनिवार्य रूप से बैंक के अधिकारियों को सौंपी जानी चाहिए।

**ग्राहक सूचना की सुरक्षा सुनिश्चित करना**

10. बैंक अपने सुचारु कामकाज के लिए ही नहीं बल्कि अपने ग्राहकों को उन्नत डिजिटल उत्पाद देने तथा विभिन्न व्यक्तिगत तथा संवेदनशील सूचनाओं को एकत्र करने की प्रक्रिया के लिए प्रौद्योगिकी पर पूरी तरह से निर्भर होते हैं। बैंकों को, इस प्रकार के डाटा के अभिरक्षक के रूप में, इसकी गोपनियता, सत्यनिष्ठा तथा उपलब्धता को संरक्षित करने के लिए उचित उपाय करने चाहिए, भले ही डाटा उनके पास हो/ ट्रांसिट में हो या ग्राहकों या तृतीयपार्टी वेंडर के पास हो; इस प्रकार की भंडारित सूचना की गोपनीयता के साथ किसी भी अवस्था में समझौता नहीं किया जाना चाहिए तथा इस प्रयोजन हेतु, बैंकों द्वारा समूचे डाटा/सूचना के जीवनचक्र में उचित प्रणालियों तथा प्रक्रियाओं को लागू करने की आवश्यकता है।

**साइबर संकट प्रबंधन योजना**

11. साइबर संकट प्रबंधन योजना (सीसीएमपी) को तुरंत शुरू करना चाहिए तथा इसे बोर्ड की अनुमोदित समग्र कार्यनीति का एक हिस्सा होना चाहिए। इस तथ्य पर विचार करते हुए कि साइबर-जोखिम अन्य कई जोखिमों से अलग है, परंपरागत बीसीपी/डीआर व्यवस्थाएँ पर्याप्त नहीं होंगी तथा साइबर-जोखिम की मात्रा को ध्यान में रखते हुए इस पर फिर से ध्यान दिए जाने की आवश्यकता है। जैसा कि आप जानते है, भारत में, सीईआरटी-इन (कंप्यूटर आपात कार्रवाई टीम-भारत, एक सरकारी संस्था) सक्रिय तथा प्रतिक्रियात्मक सेवाओं के साथ-साथ दिशानिर्देश प्रदान करते हुए, खतरे की आसूचना और वित्तीय क्षेत्रों सहित सभी क्षेत्रों में विभिन्न एजेंसियों की तैयारी का मूल्यांकन करते हुए साइबर-सुरक्षा को दुरुस्त करने में महत्वपूर्ण कदम उठा रहा है। सीईआरटी-आईएन ने राष्ट्रीय साइबर संकट प्रबंधन योजना तथा साइबर सुरक्षा मूल्यांकन फ्रेमवर्क भी तैयार किया है। सीसीएमपी बनाते समय सीईआरटी-आईएन / एनसीआईआईपीसी / आरबीआई / आईडीआरबीटी दिशानिर्देश का संदर्भ लिया जाए।

12. सीसीएमपी को निम्नलिखित चार पहलूओं पर ध्यान देना चाहिए : (i) पहचानना (ii ) जवाबी कार्रवाई (iii) सुधार तथा (iv) नियंत्रण। बैंकों को साइबर हमले को रोकने के लिए प्रभावी उपाय के साथ-साथ किसी भी साइबर-घुसपैठ का तुरंत पता लगाना भी आवश्यक है ताकि किसी अनहोनी पर जवाबी कार्रवाई/सुधारात्मक कार्रवाई/नियंत्रणात्मक कार्रवाई की जा सके। बैंकों से अपेक्षा है कि उभरते हुए साइबर हमले जैसे कि 'ज़ीरो-डे' हमले, रिमोट एक्सेस खतरे तथा इरादतन हमलों का सामना करने के लिए पूरी तरह से तैयार रहें । अन्य बातों के साथ-साथ, बैंकों को विभिन्न प्रकार के साइबर खतरों, जैसे सेवा से इंकार, डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विसेस (डीडीओएस), रेनसमवेयर/क्रिप्टोवेयर, घातक मालवेयर, व्यवसाय ई-मेल धोखाधड़ी जैसे कि स्पैम, ई-मेल फिशिंग, स्पियर फिशिंग, व्हेलिंग, विशिंग धोखाधड़ी, ड्राइव-बाय डाऊनलोड, ब्राउज़र गेटवे धोखाधड़ी, घोस्ट एडमिनिस्ट्रेटर एक्सप्लोइट्स, पहचान संबंधी धोखाधड़ी, मेमोरी अपडेट धोखाधड़ी, पासवर्ड संबंधी धोखाधड़ी से निपटने के लिए आवश्यक सुरक्षात्मक तथा सुधारात्मक उपाय करने चाहिए।

**साइबर सुरक्षा मुस्तैदी संकेतक**

13. साइबर रेसिलिएन्स फ्रेमवर्क की पर्याप्तता तथा उसके पालन का मूल्यांकन किया जाना चाहिए तथा जोखिम/मुस्तैदी के स्तर का मूल्यांकन करने के लिए संकेतकों में उतार-चढ़ाव के रूप में मापा जाना चाहिए। इन संकेतकों को स्वतंत्र अनुपालन जाँचों तथा योग्य तथा सक्षम प्रोफेसनल्स द्वारा की गई लेखा परीक्षाओं द्वारा व्यापक जांच के लिए इस्तेमाल किया जाना चाहिए। कर्मचारियों के साथ साथ हितधारकों के बीच जागरूकता को भी इस मूल्यांकन का भाग बनाया जाए।

**आरबीआई के साथ साइबर-सुरक्षा घटनाओं से संबंधित सूचनाओं को साझा/शेयर करना**

14. यह पाया गया है कि बैंक उनके द्वारा पायी गई साइबर–घटनाओं को शेयर करने में संकोच करते हैं। तथापि, वैश्विक रूप से मिले अनुभव यह दर्शाते हैं कि साइबर–घटनाओं को शेयर करने में संस्थाओं के बीच परस्पर सहयोग तथा निर्धारित प्रक्रियाओं से साइबर–जोखिमों को रोकने के लिए समय पर उपाय लागू किए जा सकेंगे। इस पर फिर गौर किया जाए कि बैंकों को सभी असामान्य साइबर–सुरक्षा के मामले रिज़र्व बैंक को रिपोर्ट करने होंगे (चाहे वे कामयाब हुए हों या फिर निष्फल प्रयास के रूप में हों)। बैंकों को प्रोत्साहित किया जाता है कि वे आईडीआरबीटी द्वारा समन्वयित उनके सीआईएससीओ फोरम की गतिविधियों में सक्रियता के साथ भाग लें तथा इन घटनाओं/मामलों को आईडीआरबीटी द्वारा स्थापित भारतीय बैंक – जोखिम तथा खतरा विश्लेषण केंद्र (आईबी-सीएआरटी) को तुरंत रिपोर्ट करें। इस प्रकार के समन्वयित प्रयासों से सामूहिक खतरे की आसूचना, समय पर अलर्ट्स तथा सक्रिय साइबर सुरक्षा उपायों को अपनाने में बैंकों को मदद मिलेगी।

**पर्यवेक्षी रिपोर्टिंग फ्रेमवर्क**

15. यह निर्णय लिया गया है कि साइबर-घटनाओं सहित सुरक्षा सूचना घटना संबंधी ब्योरे के साथ साथ सारांश स्तरीय सूचना एकत्र की जाए। बैंकों से अपेक्षा की जाती है कि घटनाओं की सूचना अनुबंध-3 में दिए गए फॉर्मेट में तुरंत दें ।

**आरबीआई को रिपोर्ट करने में मुस्तैदी में चूक का तुरंत मूल्यांकन**

16. नियंत्रणों में महत्वपूर्ण कमियों की शीघ्र पहचान की जाए तथा बोर्ड के साथ–साथ बोर्ड की आईटी उप समिति के सक्रिय मार्गदर्शन तथा पर्यवेक्षण के अंतर्गत उचित उपचारात्मक कार्रवाई को तुरंत शुरू किया जाए। अभिज्ञात कमियों, प्रस्तावित उपाय/नियंत्रण तथा उनकी प्रत्याशित प्रभावशीलता, प्रस्तावित नियंत्रण/ उपायों को कार्यान्वित करने के लिए समयसीमा के साथ माइलस्टोन तथा बैंक द्वारा अनुपालित/प्रस्तावित जोखिम मूल्यांकन तथा जोखिम प्रबंधन प्रक्रिया सहित उनकी प्रभावक्षमता का मूल्यांकन करने के लिए मापदंड को मुख्य सूचना सुरक्षा अधिकारी द्वारा 31 जुलाई 2016 तक साइबर सुरक्षा तथा सूचना प्रौद्योगिकी जांच कक्ष (सीएसआईटीई), बैंकिंग पर्यवेक्षण विभाग, केंद्रीय कार्यालय को प्रस्तुत कर दिया जाए।

**संगठनात्मक व्यवस्थाएँ**

17. बैंकों को संगठनात्मक व्यवस्थाओं की समीक्षा करनी चाहिए ताकि सुरक्षा समस्याओं का मूल्यांकन किया जाए, पर्याप्त ध्यान दिया जाए तथा तुरंत कार्रवाई करने हेतु पदक्रम के उचित स्तर तक ले जाया जाए।

**हितधारकों /शीर्ष प्रबंधन /बोर्ड के बीच साइबर-सुरक्षा जागरूकता**

18. यह गौर किया जाए कि साइबर जोखिम का प्रबंधन करने हेतु साइबर-सुरक्षित माहौल बनाने के लिए पूरे संगठन की प्रतिबद्धता आवश्यक है। इसके लिए सभी स्तरों पर स्टाफ के बीच एक उच्च स्तर की जागरूकता की आवश्यकता होगी। शीर्ष प्रबंधन तथा बोर्ड के पास खतरों की सूक्ष्मतम जानकारी होनी चाहिए तथा उन्हे उचित फेमिलियराइजेशन प्रदान किया जाना चाहिए । बैंक पूरी सक्रियता से अपने ग्राहकों, वेंडरों, सेवा प्रदाताओं तथा अन्य संबंधित हितधारकों के बीच बैंक की साइबर रेजिलिएन्स उद्देश्यों की समझ पैदा करें तथा उनके एकलयबद्ध कार्यान्वयन तथा जांच के लिए उचित कार्रवाई की अपेक्षा को सुनिश्चित करें। यह सभी जानते है कि हितधारकों (ग्राहकों, कर्मचारियों, भागीदारों तथा वेंडरों को शामिल करते हुए) को साइबर–हमले से होने वाले संभाव्य प्रभाव के बारे में जानकारी, बैंकों की साइबर सुरक्षा की तैयारी में मददगार होगी । बैंक इस संबंध में उचित कदम उठाएं । साथ ही बैंकों से यह भी अपेक्षा की जाती है कि निदेशक मण्डल तथा शीर्ष प्रबंधन में साइबर-सुरक्षा संबंधी पहलूओं पर जागरूकता, जहां आवश्यक हो, सृजन के लिए शीघ्र कदम उठाएं।

इस परिपत्र की एक प्रति आगामी बैठक में निदेशक मण्डल के समक्ष रखी जाए।

भवदीय

(आर. रविकुमार)
मुख्य महाप्रबंधक
संलग्न : यथोक्त

**Template for reporting Cyber Incidents**

1. **Security Incident Reporting (SIR) to RBI (within two to 6 hours):**
2. **Subsequent update(s) RBI (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of RBI):**

| **Basic Information** | |
|---|---|
| **1. Particulars of Reporting:** | |
| • Name of the bank | |
| • Date and Time of Reporting to RBI, CERT-IN, other agencies (please mention separately time of reporting to each) | |
| • Name of Person Reporting | |
| • Designation/Department | |
| • Contact details (e.g. official email-id, telephone no, mobile no) | |
| **2. Details of Incident:** | |
| • Date and time of incident detection | |
| • Type of incidents and systems affected<br>(i) **Outage of Critical IT system(s)** (e.g. CBS, Treasury Systems, Trade finance systems, Internet banking systems, ATMs, payment systems such as SWIFT, RTGS, NEFT, NACH, IMPS, etc.)<br>(ii) **Cyber Security Incident** *(e.g. DDOS, Ransom ware/crypto ware, data breach, data destruction, web* | |

| | |
|---|---|
| *defacement, etc.)?* ***[Please complete Annex]***<br>(iii) **Theft or Loss of Information** *(e.g. sensitive customer or business information stolen or missing or destroyed or corrupted)?*<br>(iv) **Outage of Infrastructure** *(e.g. which premises-DC/Central Processing Units, branch, etc., power/utilities supply, telecommunications supply,)?*<br>(v) **Financial** *(e.g. liquidity, bank run)?*<br>(vi) **Unavailability of Staff** (e.g. number and percentage on loss of staff /absence of staff from work (vii) **Others** *(e.g. outsourced service providers, business partners, breach of IT Act/any other law and RBI/SEBI regulations. Etc.)?* | |
| • What actions or responses have been taken by the bank at the time of first reporting/till the time of subsequent reporting? | |
| **3. Impact Assessment(examples are given but not exhaustive):** | |
| • Business impact including availability of services – Banking Services, Internet banking, Cash Management, Trade Finance, Branches, ATMs, Clearing and Settlement activities, etc. | |

| | |
|---|---|
| • Impact on stakeholders– affected retail/corporate customers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc. | |
| • Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds, etc. | |
| • Regulatory and Legal impact | |
| | |
| **4. Chronological order of events:** | |
| • Date of incident, start time and duration. | |
| • Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures | |
| • Stakeholders informed or involved | |
| • Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.) | |
| • Rationale on the decision/activation of BCP and/or DR | |
| **5. Root Cause Analysis(RCA):** | |
| • Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident | |
| • Interim measures to mitigate/resolve the issue, and reasons for taking such | |

| | |
|---|---|
| measures, and | |
| • Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected (one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident | |
| **6.** Date/target date of resolution_____ (DD/MM/YYYY). | |
| • | |
| • | |
| • | |

Note: All fields are REQUIRED to be filled unless otherwise stated.

| CYBER SECURITY INCIDENT REPORTING(CSIR) FORM | |
|---|---|
| **General Information** | **Report No:** |

1. Contact Information: *(Please provide if different from what is reported in Basic Information above)*

Name of bank:

Name of the person reporting and Designation:

Department

Official Email :

Telephone/Mobile :

2. Is this a ☐New incident ☐Update to reported incident?

- For the first update, please indicate "1. If this is an update to a reported incident, please provide the update number for this update. (X.1, X.2, X.3, X.4, etc. where X is the Report No.
  Update No: Click here to enter text.

3 What severity is this incident being classified as?

| | | |
|---|---|---|
| Severity 1 ☐<br><br>Affected critical system(s)/ customer facing applications/systems, crippled Internal network or a combination of the above | Severity 2 ☐<br><br>Incident occurred on system or network that could put the bank's network / critical system(s) or a combination of them at risk | |
| | | |

**Information about the Incident**

4. Please indicate the date and time the incident was reported to the RBI. If it is also reported to Other Agencies (CERT-IN/NCIIP), Law enforcement agencies, separately indicate the date and time of such reporting.

(Please specify in Indian Local Time (+5.30 GMT))

Reported to RBI - Date: Click here to enter a date.

Reported to CERT-IN Date: Click here to enter a date.

Reported to NCIIP Date: Click here to enter a date.

Reported to ----mention the name of agency Date: Click here to enter a date.

5. Types of Threat/Incident

((Please select more than one, as applicable)

☐ Denial of Service (DoS) ☐ Distributed Denial of Service (DDoS)

☐ Virus/Worm/Trojan/Malware ☐ Intrusion/Hack/Unauthorised access

☐ Website Defacement ☐ Misuse of Systems/Inappropriate usage

☐ APT/0-day attack ☐ Spear phishing/Whaling/Phishing/Wishing/Social engineering attack

☐ Other: Click here to enter text.

6. Is this incident related to another incident previously reported?

Choose an item.

- If “Yes”, provide more information on how both incidents are related. Click here to enter text.
- Please provide the reference no. of the previously reported incident.

Ref no: Click here to enter text.

**Incident Details**

7. Please provide details of the incident in the box below.

- When was the incident first observed/sighted/detected?
  Click here to enter a date.

- How was the incident first observed/sighted/detected?
  Click here to enter text.

- Who observed?

8. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include:

*-Location, purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc.) running on the systems/ networks, etc.*

Click here to enter text.

What security software installed on the system currently?

If known, any TCP or UDP ports involved in the incident.

If known, provide the affected system's IP address If known, provide the attacker's IP address

Where relevant, please indicate the Operating System of the affected critical system(s): Choose an item.

- If others, kindly state the OS: Click here to enter text.

9. What is the impact of the attack? (*Tick 'one' checkbox for each column*)

| Customer Service Delivery | (Loss of ) Sensitive Information | Public Confidence and Reputation |
|---|---|---|
| ☐No Impact | ☐No loss | ☐No Impact |
| ☐Minor Impact | ☐Minor Loss | ☐Minor Impact |

| | | |
|---|---|---|
| ☐Major Impact | ☐Major Loss | ☐Major Impact |
| ☐Serious Impact | ☐Serious Loss | ☐Serious Impact |
| ☐Severe Impact | ☐Severe Loss | ☐Severe impact |

10. Does the affected critical system(s)/ network(s) have potential impact to another critical system/critical asset(s) of the bank?

Choose an item.

- If "Yes", please provide more details.

Click here to enter text.

**Incident Status**

11. What is/are the type(s) of follow up action(s) that has/have been taken at this time?

Click here to enter text.

12. What is the current status or resolution of this incident?

Choose an item.

If it is not resolved, what is the next course of actions?

Click here to enter text.

13. What is the earliest known date of attack or compromise? *(Tick 'checkbox' if unknown)*

(Please specify in Indian Local Time +5.30 GMT)

Date: Click here to enter a date. Unknown: ☐

14. What is the source/cause of the incident? *('NIL' OR 'NA' if unknown)*

Click here to enter text.

15. Has the incident been reported to CERT-IN/NCIIP/ any law enforcement agency/IBCART? Choose an item.

- If "Yes", specify the agency that is being reported to.

Click here to enter text..

16. Is chain of custody maintained?

17. Has the bank filled chain of custody form?

18. What tools were used for collecting the evidence for the incident?

**: Attack Vectors**

E1. Did the bank locate/identify IP addresses**, domain names, related to the incident**

Whether the Indicators of Compromise, list of IP addresses identified from the incident, involvement of the IP addresses in the incident (ex. Victim, Malware Command & Control Servers, etc.), domain names resolved, involvement of the domain names in the incident. (ex. Drive-by-download Servers, Malware Control & Command Servers, defaced website), email addresses identified and their involvement, malicious files/attachments (file name, size, MD5/SHA1 hash, etc. ) etc. have been reported in IB-CART/CERT-IN/NCIIP/Law enforcement agencies

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# अधिसूचनाएं

**ग्राहक संरक्षण - अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन में ग्राहकों की देयता को सीमित करना**

भा.रि.बैं./2017-18/15
बैंविवि.सं.एलईजी.बीसी.78/09.07.005/2017-18

6 जुलाई, 2017

सभी अनुसूचित वाणिज्यिक बैंक (क्षेत्रीय ग्रामीण बैंकों को छोड़कर)
सभी लघु वित्त बैंक और भुगतान बैंक

महोदय/ महोदया,

**ग्राहक संरक्षण - अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन में ग्राहकों की देयता को सीमित करना**

कृपया धोखाधड़ी या अन्य प्रकार के लेनदेनों से उत्पन्न गलत नामे का प्रत्यावर्तन के संबंध में दिनांक 8 अप्रैल, 2002 का हमारा परिपत्र बैंपविवि.एलईजी.बीसी.86/09.07.007/2001-02 देखें।

2. वित्तीय समावेशन और ग्राहक सुरक्षा पर दिए जा रहे अधिक जोर के कारण और अनधिकृत लेनदेनों, जिसके परिणामस्वरूप ग्राहकों के खातों/ कार्डों के नामे डालने से संबंधित ग्राहकों की शिकायतों में हाल ही में हुई तीव्र वृद्धि को देखते हुए, इन परिस्थितियों में ग्राहक की देयता निर्धारित करने के मानदंड की समीक्षा की गई है। इस संबंध में संशोधित निदेश नीचे दिए गए हैं।

**प्रणालियों और प्रक्रियाओं को मजबूत बनाना**

3. मोटे तौर पर, इलेक्ट्रॉनिक बैंकिंग लेनदेन को दो श्रेणियों में विभक्त किया जा सकता है:

i. दूरस्थ/ ऑनलाइन भुगतान लेनदेन (ऐसे लेनदेन जिनमें लेनदेन करते समय प्रस्तुत किए जाने वाले वास्तविक भुगतान लिखतों की आवश्यकता नहीं होती, उदाहरणार्थ इंटरनेट बैंकिंग, मोबाइल बैंकिंग, कार्ड मौजूद नहीं (सीएनपी लेनदेन), प्री-पेड भुगतान लिखत (पीपीआई), और

ii. आमने-सामने/ सामीप्य भुगतान लेनदेन (ऐसे लेनदेन जिनमें लेनदेन करते समय कार्ड अथवा मोबाइल फोन जैसे भौतिक भुगतान लिखत, उदाहरणार्थ एटीएम, पीओएस, इत्यादि को प्रस्तुत करने की आवश्यकता होती है।)

4. बैंकों में प्रणालियों और प्रक्रियाओं को इस प्रकार बनाया जाए कि इलेक्ट्रॉनिक बैंकिंग लेनदेन करते समय ग्राहक सुरक्षित महसूस करें। उक्त को साकार करने के लिए, बैंक निम्न को तैयार करेंगे:

i. ग्राहकों द्वारा किए जाने वाले इलेक्ट्रॉनिक बैंकिंग लेनदेन की सुरक्षा और संरक्षा सुनिश्चित करने के लिए उचित प्रणालियां और प्रक्रियाएं;

ii. धोखाधड़ी का पता लगाने और उसे रोकने के लिए सुदृढ़ और गतिशील प्रणाली;

iii. अनधिकृत लेनदेन से उत्पन्न जोखिम (उदाहरण के लिए, बैंक की मौजूदा प्रणाली में कमियां) का मूल्यांकन करने और ऐसी घटनाओं से उत्पन्न देयताओं को मापने के लिए प्रणाली;

iv. जोखिम कम करने और उनसे उत्पन्न होने वाली देयताओं के प्रति स्वयं का संरक्षण करने के लिए समुचित उपाय; और

v. ग्राहकों को लगातार और बार-बार यह सूचित करने की प्रणाली कि इलेक्ट्रॉनिक बैंकिंग और भुगतान संबंधी धोखाधड़ी से स्वयं को सुरक्षित कैसे रखें।

**ग्राहकों द्वारा बैंकों को अनधिकृत लेनदेन की रिपोर्टिंग**

5. बैंक अपने ग्राहकों को एसएमएस चेतावनी के लिए अनिवार्य रूप से पंजीकृत होने के लिए और जहां कहीं उपलब्ध हो, ई-मेल चेतावनी, इलेक्ट्रॉनिक बैंकिंग लेनदेन के लिए पंजीकृत होने के लिए कहें। एसएमएस चेतावनी ग्राहकों को अनिवार्य रूप से भेजी जाएगी, जबकि ई-मेल चेतावनी, जहां पंजीकृत हो, को ही भेजी जाए। ग्राहकों को यह अवश्य सूचित किया जाए कि वे किसी अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन के बाद यथाशीघ्र अपने बैंक को अधिसूचित करें। उन्हें यह भी सूचित किया जाए कि बैंक को सूचना देने में जितना अधिक समय लगेगा, बैंक/ग्राहक को नुकसान का जोखिम उतना ही अधिक होगा। इसे सुविधाजनक बनाने के लिए, बैंक विभिन्न माध्यमों (कम-से-कम, वेबसाइट, फोन बैंकिंग, एसएमएस, ई-मेल, आईवीआर, समर्पित टोल-फ्री हेल्पलाइन, गृह शाखा को रिपोर्ट करना, इत्यादि) से ग्राहकों को 24x7 पहुंच प्रदान करें, ताकि वे अनधिकृत लेनदेनों और/ अथवा कार्ड, इत्यादि जैसे भुगतान लिखतों के खो जाने अथवा चोरी हो जाने की सूचना दे सकें। बैंक ग्राहकों को एसएमएस और ई-मेल चेतावनी के "उत्तर" द्वारा तुरन्त प्रतिक्रिया देने की सुविधा भी देंगे और ग्राहकों को आपत्ति, यदि कोई हो, को दर्ज कराने के लिए किसी वेब पेज अथवा किसी ई-मेल पते को ढूंढने की आवश्यकता नहीं पड़नी चाहिए। इसके अतिरिक्त, अनधिकृत इलेक्ट्रॉनिक लेनदेन को रिपोर्ट करने के विशिष्ट विकल्प सहित, शिकायत दर्ज करने का सीधा लिंक बैंक द्वारा उनकी वेबसाइट के होम पेज पर उपलब्ध कराया जाएगा। खो जाने/ धोखाधड़ी की सूचना देने की प्रणाली में यह भी सुनिश्चित किया जाएगा कि ग्राहकों को तुरंत उत्तर (स्वतः उत्तर सहित) शिकायत प्राप्त होने की सूचना देते हुए दर्ज शिकायत संख्या सहित दिया जाए। चेतावनी भेजने और उनकी प्रतिक्रिया प्राप्त करने के लिए बैंकों द्वारा प्रयुक्त संचार प्रणाली में संदेश भेजने का समय और तारीख एवं उस पर ग्राहक की प्रतिक्रिया, यदि कोई हो, की प्राप्ति रिकार्ड होना आवश्यक है। यह ग्राहक की देयता की सीमा निर्धारित करने में महत्वपूर्ण होगा। बैंक को मोबाइल नंबर उपलब्ध न कराने वाले ग्राहकों को बैंक एटीएम नकदी आहरण को छोड़कर इलेक्ट्रॉनिक लेनदेन की सुविधा प्रदान न करें। ग्राहक से अनधिकृत लेनदेन की रिपोर्ट प्राप्त होने पर, बैंक उस खाते में और अधिक अनधिकृत लेनदेन रोकने के लिए तत्काल कदम उठाएं।

**ग्राहक की सीमित देयता**

**(क) ग्राहक की शून्य देयता**

6. किसी ग्राहक की शून्य देयता की पात्रता वहां उत्पन्न होगी जहां अनधिकृत लेनदेन निम्नलिखित मामलों में होता है:

i. बैंक की ओर से अंशदायी धोखाधड़ी/ लापरवाही/ कमी (इस पर ध्यान दिए बगैर कि ग्राहक द्वारा लेनदेन को रिपोर्ट किया गया है या नहीं)।

ii. अन्य पक्ष द्वारा उल्लंघन जहां न तो बैंक की ओर से कमी हुई हो, न ही ग्राहक की ओर से, बल्कि प्रणाली में ही कहीं कमी हो, और ग्राहक अनधिकृत लेनदेन के संबंध में बैंक से सूचना प्राप्त होने के **तीन कार्य दिवसों के भीतर** बैंक को सूचित कर देता है।

**(ख) ग्राहक की सीमित देयता**

7. कोई ग्राहक निम्नलिखित मामलों में अनधिकृत लेनदेन के कारण होने वाले नुकसान के लिए उत्तरदायी होगा:

i. ऐसे मामले जिनमें हानि किसी ग्राहक की लापरवाही के कारण हुई है, जैसे जहां उसने भुगतान संबंधी गोपनीय जानकारी साझा की है, वहां ग्राहक को सम्पूर्ण नुकसान तब तक वहन करना होगा जब तक कि वह अनधिकृत लेनदेन की सूचना बैंक को न दे दे। अनधिकृत लेनदेन की सूचना प्राप्ति के बाद होने वाला कोई भी नुकसान बैंक द्वारा वहन किया जाएगा।

ii. ऐसे मामले जिनमें अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन की जवाबदेही न तो बैंक की हो, न ही ग्राहक की, बल्कि कहीं-न-कहीं प्रणाली की ही हो, और जहां इस प्रकार की लेनदेन की सूचना बैंक को देने में ग्राहक की ओर से विलम्ब (बैंक से सूचना प्राप्ति के बाद **चार से सात कार्य दिवसों** का) हो, वहां ग्राहक की प्रति लेनदेन देयता लेनदेन मूल्य अथवा सारणी 1 में उल्लिखित राशि, जो भी कम हो, तक सीमित रहेगी।

| **सारणी 1** | |
|---|---|
| **पैराग्राफ 7 (ii) के अंतर्गत ग्राहक की अधिकतम देयता** | |
| **खाते का प्रकार** | **अधिकतम देयता (₹)** |
| • बीएसबीडी खाते | 5,000 |
| • अन्य सभी बचत बैंक खाते<br>• पूर्व-प्रदत भुगतान लिखत और गिफ्ट कार्ड<br>• एमएसएमई के चालू/ नकदी ऋण/ ओवरड्राफ्ट खाते<br>• व्यक्तियों के वार्षिक औसत जमाशेष वाले (धोखाधड़ी की घटना से पहले 365 दिनों के दौरान)/ 25 लाख रुपये तक की सीमा वाले चालू/ नकदी ऋण/ ओवरड्राफ्ट खाते<br>• 5 लाख रुपये तक की सीमा वाले क्रेडिट कार्ड | 10,000 |
| • अन्य सभी चालू/ नकदी ऋण/ ओवरड्राफ्ट खाते<br>• 5 लाख रुपये से अधिक की सीमा वाले क्रेडिट कार्ड | 25,000 |

इसके अतिरिक्त, यदि रिपोर्ट करने में **सात कार्य दिवसों** से अधिक समय का विलम्ब होता है तो ग्राहक की देयता बैंक के बोर्ड द्वारा अनुमोदित नीति के अनुसार निर्धारित की जाएगी। ग्राहक की देयता के संबंध में इन निदेशों के अनुपालन में बनाई गई अपनी नीति के ब्योरे बैंक खाता खोलते समय ग्राहकों को प्रदान करेंगे। बैंक पब्लिक डोमेन में अपनी अनुमोदित नीति को व्यापक प्रचार-प्रसार के लिए प्रदर्शित भी करेंगे। मौजूदा ग्राहकों को भी बैंक की नीति के बारे में व्यक्तिगत रूप से सूचित किया जाएगा।

8. उपर्युक्त पैरा 6 (ii) और पैरा 7 (ii) में दिए गए अनुसार, अन्य पक्ष द्वारा उल्लंघन के मामले में ग्राहक की सम्पूर्ण देयता, जहां न तो बैंक की ओर से कमी हुई हो, न ही ग्राहक की ओर से, बल्कि प्रणाली में ही कहीं कमी हो, का सारांश सारणी 2 में दिया गया है:

| **सारणी 2** | |
|---|---|
| **ग्राहक की देयता का सारांश** | |
| **धोखाधड़ीपूर्ण लेनदेन की सूचना प्राप्त होने की तिथि से उसे रिपोर्ट करने में लगा समय** | **ग्राहक की देयता (₹)** |
| 3 कार्यदिवसों के भीतर | शून्य देयता |
| 4 से 7 कार्यदिवसों के भीतर | लेनदेन की कीमत अथवा सारणी 1 में उल्लिखित राशि, जो भी कम हो |
| 7 कार्यदिवसों से अधिक समय | बैंक के बोर्ड द्वारा अनुमोदित नीति के अनुसार |

सारणी 2 में उल्लिखित कार्यदिवसों की संख्या की गणना सूचना प्राप्त होने की तिथि को छोड़कर ग्राहक की गृह शाखा की कार्य समयसारणी के अनुसार की जाएगी।

**ग्राहक की शून्य देयता/ सीमित देयता के लिए प्रतिवर्ती समय-सीमा**

9. ग्राहक द्वारा सूचित किए जाने पर, बैंक अनधिकृत इलेक्ट्रॉनिक लेनदेन में शामिल राशि को ग्राहक द्वारा ऐसी सूचना देने की तिथि से 10 कार्यदिवसों के भीतर ग्राहक के खाते में जमा (प्रतिवर्ती कार्रवाई) करेगा (बीमा दावे, यदि कोई हो, के निपटान की प्रतीक्षा किए बिना)। बैंक ग्राहक की लापरवाही के मामलों में भी अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन के मामले में किसी ग्राहक की देयता को अपने विवेक से छूट देने का भी निर्णय ले सकते हैं। जमा राशि की कीमत वही होगी जो अनधिकृत लेनदेन की तिथि के अनुसार होगी।

10. इसके अतिरिक्त, बैंक यह सुनिश्चित करेंगे कि :

i. शिकायत का निराकरण किया गया है और ग्राहक की देयता, यदि कोई हो, जो बैंक के बोर्ड द्वारा अनुमोदित नीति में विनिर्दिष्ट किए गए समय के भीतर, परन्तु शिकायत प्राप्त होने की तिथि से 90 दिनों के भीतर, निर्धारित की गई हो और ग्राहक को उपर्युक्त पैरा 6 से 9 के प्रावधानों के अनुसार क्षतिपूर्ति दी गई है;

ii. जहां 90 दिनों के भीतर शिकायत का निराकरण कर पाना अथवा ग्राहक की देयता, यदि कोई हो, निर्धारित कर पाना संभव नहीं है, वहां पैरा 6 से 9 में निर्धारित क्षतिपूर्ति ग्राहक को अदा की गई है; और

iii. डेबिट कार्ड/ बैंक खाते के मामले में, ग्राहक को ब्याज का नुकासान न सहन करना पड़े, और क्रेडिट कार्ड के मामले में, ग्राहक को ब्याज का अतिरिक्त बोझ वहन न करना पड़ता हो।

**ग्राहक संरक्षण के लिए बोर्ड द्वारा अनुमोदित नीति**

11. ग्राहक की लापरवाही/ बैंक की लापरवाही/ बैंकिंग प्रणाली संबंधी धोखाधड़ी/ अन्य पक्ष संबंधी उल्लंघन के कारण ग्राहक के खातों में अनधिकृत रूप से नामे डाले जाने से उत्पन्न जोखिम को ध्यान में रखते हुए, बैंकों के लिए यह आवश्यक है कि वह निर्दिष्ट परिदृष्यों में अनधिकृत लेनदेन के मामले में ग्राहकों के अधिकार और दायित्वों को स्पष्ट रूप से परिभाषित करें। बैंक अपने बोर्ड के अनुमोदन से अपनी ग्राहक संबंध नीति बनाए/ संशोधित करें, जिसमें इलेक्ट्रॉनिक बैंकिंग लेनदेन में शामिल जोखिम और दायित्व के संबंध में ग्राहक जागरूकता सृजित करने और अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन के ऐसे मामलों में ग्राहक की देयता तय करने की प्रणाली सहित ग्राहक सुरक्षा के पहलू शामिल हों। उक्त नीति पारदर्शी, भेदभाव रहित होनी चाहिए और उसमें अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन के लिए ग्राहकों को क्षतिपूर्ति की प्रणाली निर्धारित की गई हो और उसमें उपर्युक्त पैरा 10 में निहित अनुदेशों को ध्यान में रखते हुए ऐसी क्षतिपूर्ति प्रदान करने के लिए समय-सीमा भी निर्धारित हो। उक्त नीति को शिकायत से निपटने/ वृद्धि प्रक्रिया के ब्यौरे के साथ बैंक की वेबसाइट पर प्रदर्शित किया जाएगा। इस परिपत्र में शामिल अनुदेशों को नीति में समाहित किया जाएगा।

**प्रमाण का दायित्व**

12. अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन के मामले में ग्राहक की देयता को सिद्ध करने का दायित्व बैंक के ऊपर होगा।

**रिपोर्टिंग और निगरानी संबंधी अपेक्षाएं**

13. बैंक बोर्ड को अथवा इसकी किसी समिति को ग्राहक देयता मामले की रिपोर्टिंग करने के लिए उचित प्रणाली और संरचना तैयार करेंगे। रिपोर्टिंग में, अन्य बातों के साथ, मामलों की मात्रा/ संख्या और शामिल समग्र मूल्य मामले की विभिन्न श्रेणियों जैसे, कार्ड की मौजूदगी में लेनदेन, कार्ड की गैर-मौजूदगी में लेनदेन, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, एटीएम लेनदेन इत्यादि के बीच वितरण शामिल होंगे। प्रत्येक बैंक में ग्राहक सेवा पर स्थायी समिति ग्राहकों या अन्य द्वारा रिपोर्ट किए गए अनधिकृत इलेक्ट्रॉनिक बैंकिंग

लेनदेन के साथ-साथ, इस संबंध में की गई कार्रवाई और शिकायत निराकरण प्रणाली के कार्य की समय-समय पर समीक्षा करेगी और प्रणाली ओर प्रक्रिया में सुधार के लिए उचित कदम उठाएगी। ऐसे सभी लेनदेनों की समीक्षा बैंक के आंतरिक लेखापरीक्षकों द्वारा की जाएगी।

14. इस परिपत्र में दिए गए अनुदेश बैंकों के क्रेडिट कार्ड, डेबिट कार्ड तथा रुपए में मूल्यवर्गित को-ब्रांडेड प्री-पेड कार्ड तथा क्रेडिट कार्ड जारीकर्ता एनबीएफसी के परिचालन पर दिनांक 1 जुलाई, 2015 के हमारे मास्टर परिपत्र बैंविवि.सं.एफएसडी. बीसी.18/24.01.009/2015-16 में दिए गए कुछ अनुदेशों को अनुबंध में दिए गए अनुसार अधिक्रमित करते हैं।

भवदीय,

(प्रकाश बलियारसिंह)
मुख्य महाप्रबंधक

**अनुबंध**

**बैंकों तथा क्रेडिट कार्ड जारीकर्ता एनबीएफसी के क्रेडिट कार्ड, डेबिट कार्ड तथा रुपए में मूल्यवर्गित को-ब्रांडेड प्री-पेड कार्ड परिचालन पर हमारे मास्टर परिपत्र (दिनांक 1 जुलाई, 2015 का बैंविवि.सं.एफएसडी. बीसी.18/24.01.009/2015-16) में दिए गए अनुदेश जिन्हें अनुसूचित वाणिज्यिक बैंकों के संबंध में संशोधित किया जाता है**

| क्र. सं. | मौजूदा अनुदेश | | इस परिपत्र में संशोधित अनुदेश (पैरा सं.) |
|---|---|---|---|
| | पैरा सं. | अनुदेश | |
| 1 | I.14.1 | बैंकों /गैर- बैंकिंग वित्तीय कंपनियों को चाहिए कि वे धोखाधड़ी से निपटने के लिए आंतरिक नियंत्रण प्रणाली स्थापित करें और धोखाधड़ी निवारक समितियों/ टास्क फोर्स में सक्रिय रूप से भाग लें, ये समितियां /टास्क फोर्स धोखाधड़ी रोकने और धोखाधड़ी नियंत्रण तथा कार्यान्वयन संबंधी पूर्वयोजित उपाय करने के लिए कानून बनाती हैं। | 4 |
| 2 | II.7.(viii) (ग) | 7. ग्राहकों को कार्ड जारी करने की निबंधन और शर्तें:<br>(viii) (ग) इन शर्तों के द्वारा कार्डधारक बाध्य होगा कि वह निम्नलिखित के संबंध में जानकारी मिलते ही अविलंब बैंक को सूचित करेगा:<br>- कार्ड के खो जाने, चोरी होने या उसकी नकल बनाए जाने या अन्य साधनों से उसका दुरुपयोग होने पर,<br>- कार्डधारक के खाते में किसी अनधिकृत लेनदेन दर्ज होने पर,<br>- बैंक द्वारा उस खाते के परिचालन में किसी प्रकार की त्रुटि या अनियमितता होने पर। | 5 |
| 3 | II.7.(viii) (घ) | (viii) (घ): इन शर्तों में ऐसे संपर्क केंद्र को विनिर्दिष्ट किया जाएगा जहां ऐसी सूचना दी जा सके। ऐसी सूचना दिन या रात में किसी भी समय दी जा सकेगी। | 5 |
| 4 | II.7.(x) | इन शर्तों में यह विनिर्दिष्ट किया जाएगा कि किसी कार्डधारक को किसी प्रणालीगत खराबी के कारण हुई प्रत्यक्ष हानि के लिए, जो बैंक के प्रत्यक्ष नियंत्रण में हो, बैंक उत्तरदायी होगा। तथापि, भुगतान प्रणाली के तकनीकी रूप से खराब हो जाने के कारण हुई किसी क्षति के लिए बैंक को जिम्मेदार नहीं ठहराया जाएगा यदि प्रणाली के खराब होने की जानकारी उपकरण के डिसप्ले पर किसी संदेश द्वारा या किसी अन्य माध्यम से कार्डधारक को दी गयी हो। लेनदेन पूरा न होने या गलत लेनदेन होने की स्थिति में बैंक की जिम्मेदारी शर्तों पर लागू होने वाले कानून के प्रावधानों के अधीन मूलधन राशि तथा नुकसान हुए ब्याज तक सीमित है। | 6 एवं 7 |
| 5 | II.9.(i) | बैंक डेबिट कार्ड की पूर्ण सुरक्षा सुनिश्चित करेगा। डेबिट कार्डकी सुरक्षा की जिम्मेदारी बैंक की होगी तथा सुरक्षा में चूक होने या सुरक्षा प्रणाली के फेल होने के कारण किसी पक्ष को होनेवाली हानि का वहन बैंक को करना होगा। | 4, 6 एवं 7 |
| 6 | II.9.(iv) | iv) कार्डधारक कार्ड के खोने, चोरी होने या उसकी नकल बनाए जाने की सूचना बैंक को देने तक हुई हानि का वहन करेगा, किन्तु केवल एक निश्चित सीमा (जिस पर बैंक तथा कार्डधारक के बीच पहले से ही लेनदेन के प्रतिशत या एक निश्चित राशि के रूप में समझौता हुआ होगा) तक ही करेगा सिवाय ऐसे मामले को छोड़कर जहां कार्डधारक ने कपटपूर्ण रीति से, जानबूझकर या अत्यधिक लापरवाही से कार्य किया हो। | 6 एवं 7 |
| 7 | II.9.(v) | प्रत्येक बैंक ऐसे साधन मुहैया कराएगा जिनसे ग्राहक दिन या रात के किसी भी समय अपने भुगतान साधनों के खोने, चोरी हो जाने या उसकी नकल बनाए जाने के संबंध में सूचना दे सके। | 5 |
| 8 | II.9.(vi) | कार्ड के खोने, चोरी हो जाने या उसकी नकल बनाए जाने के संबंध में सूचना प्राप्त होने पर बैंक ऐसी सभी संभव कार्रवाइयां करेगा जिनसे कार्ड का आगे प्रयोग किया जा सके। | 5 |

/

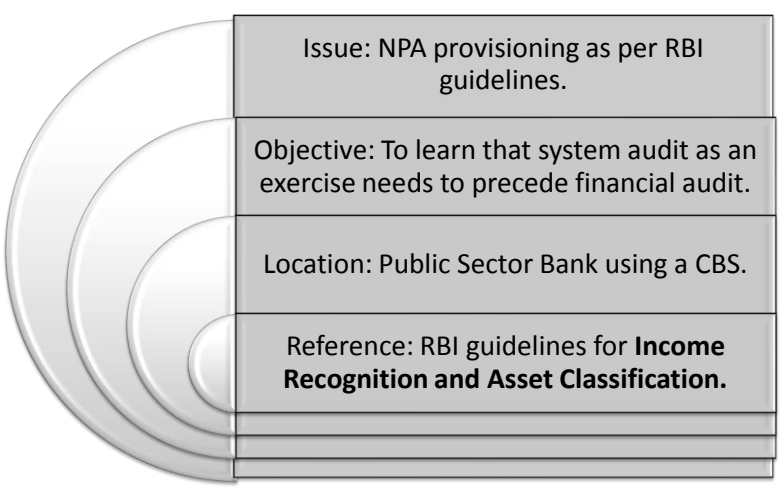
# What is IS Audit?

3. It focuses on determining the risks that are relevant to information assets, and

4. In assessing controls in order to reduce or mitigate these risks.

# Why IS Audit?

Case to highlight the above point:




2

# Why IS Audit?

Specific Point: Provision to be made for sub-standard assets, where the advance as per nature is unsecured.

The guidelines state that a provision of @25% has to be made of total out-standing.

This is an exception to general rule of provision @15%. The exception is created as the advance is basically **unsecured in nature. CREDIT CARD**

3

# What is IS Audit?

1. It is an examination of the controls within an Information technology (IT) infrastructure.

2. It is the process of collecting and evaluating the evidence of an organization's information systems, practices, and operations.

4

# How to perform IS Audit?

The fundamental principles of audit remain the same.

IS audit like financial audit, focuses on the risk arising from inadequate or inefficient controls.

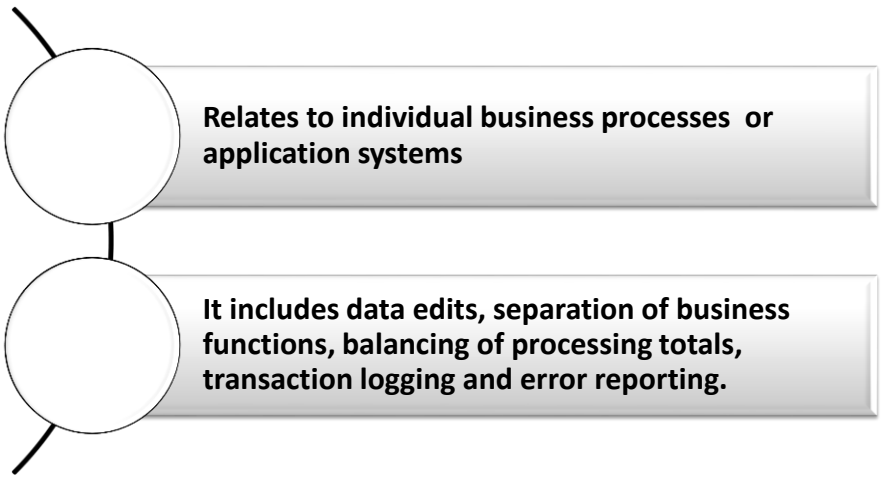
The change is in perspective and approach.

5

# Types of Control

- Preventive Control
- Detective Control
- Corrective Control
- Input Control
- Processing Control
- Output Control

## Application Controls




7

## Application Control: General Objectives


8

## Application Control: COBIT Definition

COBIT states that; application controls are intended to provide reasonable assurance that management's objectives relative to a given application have been achieved..

9

## Application Controls: Objectives as defined by COBIT

- Source Data Preparation and Authorisation
- Source Data Collection and Entry
- Accuracy, Completeness and Authenticity Checks
- Processing Integrity and Validity
- Output Review, Reconciliation and Error Handling
- Transaction Authentication and Integrity during transmission

10

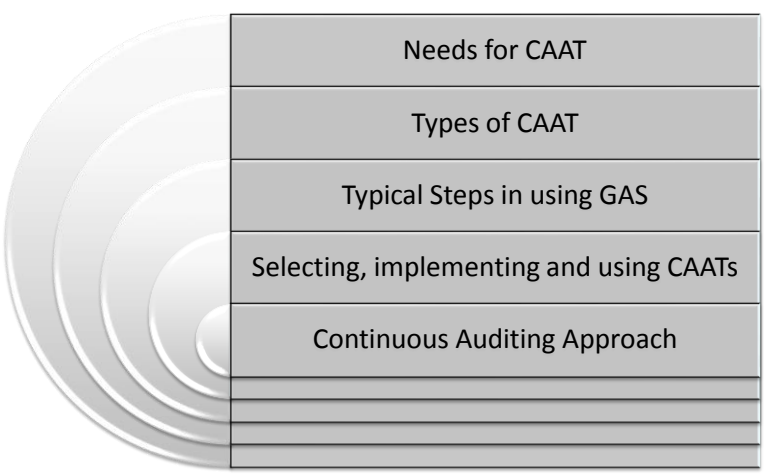
## Computer Assisted Audit Techniques

**CAAT is a significant tool for auditors to gather evidences independently.**

1. It provides a mean to gain access and to analyse data for a predetermined audit objective, and
2. Report the audit findings with evidences.
3. It helps the auditor to obtain evidence directly on the quality of records produced and maintained in the system.

11

## Computer Assisted Audit Techniques




12

## Needs for CAAT

1. For evidence collections

2. Analysis and interpretation of this evidence.

3. E-form evidence can only be verified using CAAT.

13

## Types of CAAT

Use the audit software developed by the client

Design and develop his own audit software

Use a standard off the shelf Generalised Audit Software

14

राष्ट्रीय कृषि और ग्रामीण विकास बैंक
पर्यवेक्षण विभाग
प्रधान कार्यालय : बीकेसी, बान्द्रा (पू), मुम्बई - 400 051
दूरभाष : +91 22 2654 1834 • फैक्स : +91 22 2653 0103
ई-मेल : dos@nabard.org • वेबसाईट : www.nabard.org

National Bank for Agriculture and Rural D
Department of Supervision
Head Office : BKC, Bandra (E), Mumbai - 400 051
Tel. : +91 22 2654 1834 • Fax : +91 22 2653 0103
E-mail : dos@nabard.org • Website : www.nabard.org

संदर्भ सं.राबैं.डॉस.एचओ.पॉल/ 3634 /जे-1/ 2014-15
25 फरवरी 2015 (परिपत्र सं.33 /डॉस 01 / 2015 )



अध्यक्ष, सभी क्षेत्रीय ग्रामीण बैंक
प्रबंध निदेशक, सभी राज्य सहकारी बैंक
प्रबंध निदेशक/ मुख्य कार्यपालक अधिकारी, सभी मध्यवर्ती सहकारी बैंक

महोदया/ प्रिय महोदय

**सूचना प्रणाली (आईएस) अंकेक्षण का प्रारंभ**

जैसा कि आप जानते हैं, हाल के समय में बैंकों और वित्तीय संस्थाओं द्वारा प्रौद्योगिकी अपनाने में महत्वपूर्ण वृद्धि हुई है और प्रौद्योगिकीय नवोन्मेष दूरदराज के लोगों तक वित्तीय सेवाएं पहुंचाने के लिए एक महत्वपूर्ण उपकरण बन गया है. ग्रामीण लोगों को बैंकिंग और अन्य वित्तीय सेवाएं देने में पारदर्शिता और सुरक्षा बनाए रखने के लिए तथा प्रौद्योगिकी अपनाने से उत्पन्न होने वाली जोखिम को कम करने के लिए भी ग्रामीण वित्तीय संस्थाओं यथा क्षेग्रा बैंकों और सहकारी बैंकों में सूचना प्रणाली अंकेक्षण (आईएस ऑडिट) शुरू करने की बहुत अधिक आवश्यकता है.

2. क्षेग्रा बैंकों और सहकारी बैंकों के, बैंकिंग परिचालनों के लिए कोर बैंकिंग सोल्यूशन सिस्टम में स्थानांतरण (माइग्रेशन) और ग्राहकों को बैंकों द्वारा विभिन्न उत्पाद इलेक्ट्रॉनिक रूप में प्रस्तावित किए जाने के परिणामस्वरूप सूचना प्रणाली की संरक्षा और सुरक्षा को सुनिश्चित करने के लिए वर्तमान आंतरिक नियंत्रण प्रणाली की हमने समीक्षा की. यह पाया गया कि कुछ बैंक आंतरिक लेखापरीक्षा/ निरीक्षण के एक भाग के रूप में सूचना प्रणाली अंकेक्षण की शुरूआत कर चुके हैं , जबकि कुछ अन्य बैंकों द्वारा सूचना प्रणाली अंकेक्षण की शुरूआत की जानी है. अतः यह निर्णय लिया गया है कि बैंकों के लिए विस्तृत दिशानिर्देश जारी किये जाए ताकि वे उपयुक्त सूचना प्रणाली अंकेक्षण तंत्र को क्रियाशील कर सकें.

3. चूंकि बैंकिंग प्रणाली आईटी परिवेश में स्थानांतरित (माइग्रेट) कर गया है, इसलिए प्रत्येक बैंक की अपनी उपयुक्त और मजबूत आईटी नीति और सूचना प्रणाली अंकेक्षण का होना आवश्यक है. सूचना प्रणाली अंकेक्षण यह निर्धारित करने के लिए, कि क्या सूचना प्रणाली आस्तियों को सुरक्षा प्रदान करता है, आंकडों की विश्वसनीयता को बनाए रखता है, बैंक की

आइटी नीति को ध्यान में रखते हुए संगठनात्मक लक्ष्य को प्रभावी और सक्षम रूप से प्राप्त करता है, साक्ष्य संकलन और मूल्यांकन की प्रक्रिया है। सूचना प्रणाली अंकेक्षण एक नियोजित प्रक्रिया है जो जांच आधार पर की जाती है./ सूचना प्रणाली अंकेक्षण का प्रमुख उद्देश्य यह सुनिश्चित करना है कि (i) सूचना प्रणाली, जिस पर बैंक की निर्भरता बहुत अधिक है, आवश्यकता पर हर वक्त व्यवसाय के लिए उपलब्ध रहता है (ii) ये प्रणाली सभी प्रकार की क्षति और आपदाओं से संरक्षित है (iii) सूचना प्रणाली का खुलासा, केवल उन्हीं जो इसे देखने और उपयोग करने के लिए प्राधिकृत हैं, को किया जाता है और किसी अन्य के लिए नहीं (iv) इस प्रणाली द्वारा प्रदान की गई सूचना हमेशा परिशुद्ध व विश्वसनीय है और ठीक समय पर उपलब्ध है (v) प्रबंधन द्वारा यह सुनिश्चित करने के लिए, कि इस प्रणाली के आंकड़े और सॉफ्टवेयर में किसी प्रकार का अनधिकृत संशोधन नहीं किया जा सके, उपयुक्त उपाय किए गए हैं. इस प्रकार सूचना प्रणाली अंकेक्षण में भौतिक और पर्यावरणीय समीक्षा, सिस्टम प्रशासनिक (एडमिनिस्ट्रेशन) समीक्षा; एप्लिकेशन सॉफ्टवेयर समीक्षा, नेटवर्क सुरक्षा समीक्षा, व्यवसाय निरंतरता समीक्षा, आंकड़े विश्वसनीय समीक्षा इत्यादि शामिल है/

4. सूचना प्रणाली अंकेक्षण के लिए विस्तृत दिशानिर्देश अनुबंध ए और सूचना प्रणाली अंकेक्षण करने वाले लेखापरीक्षक के दिशानिर्देश हेतु जांच सूची अनुबंध ए(i) में सूचनार्थ दिए गए हैं. यद्यपि सूचना प्रणाली अंकेक्षण की निदर्शी विषय क्षेत्र अनुबंध बी में दी गई हैं, सूचना सुरक्षा, इलेक्ट्रॉनिक बैंकिंग, प्रौद्योगिकी जोखिम प्रबंधन और साइबर धोखाधड़ी से संबंधित दिशानिर्देश अनुबंध बी (i) में दिए गए हैं.

5. उक्त को ध्यान में रखते हुए, यह सूचित किया जाता है कि:

i. बैंक अपने कम्प्यूटरीकरण स्तर/ अपनाई गई सीबीएस प्रणाली के लिए उपयुक्त सूचना प्रणाली अंकेक्षण नीति (यदि अभी तक नहीं अपनाई गई है) , निदेशक मंडल के अनुमोदन से अपनाए और बैंकिंग उद्योग की सर्वोत्तम प्रथा के अनुरूप और भारतीय रिजर्व बैंक/ नाबार्ड द्वारा समय-समय पर जारी निर्देश के अनुसार नियमित अंतराल पर इसकी समीक्षा करे.

ii. चूंकि अधिकांश बैंक हाल के वर्षों में ही सीबीएस में माइग्रेट हो गए हैं/ सीबीएस में माइग्रेट होने की प्रक्रिया में हैं, वे सबसे पहले यह सुनिश्चित करें कि किसी अर्हता प्राप्त फर्म द्वारा " माइग्रेशन ऑडिट" तुरंत पूरा किया जाता है .

iii. बैंक किसी अर्हता प्राप्त लेखापरीक्षा फर्म द्वारा या सक्षम सूचना प्रणाली कार्मिक दल द्वारा वार्षिक आधार पर सूचना प्रणाली अंकेक्षण करने के लिए उपयुक्त प्रणाली और प्रक्रिया अपनाए जिसमें सभी अति महत्वपूर्ण (व्यवसाय के स्वरूप और आकार के अनुसार) शाखाएं और प्रधान कार्यालय/ नियंत्रक कार्यालय के कार्य शामिल हों.

iv. इस प्रकार की लेखापरीक्षा सांविधिक लेखापरीक्षा से पहले की जानी चाहिए ताकि सांविधिक लेखापरीक्षकों को जांच और लेखापरीक्षा रिपोर्ट में अपनी टिप्पणी, यदि कोई हो, में शामिल करने के लिए, सूचना प्रणाली अंकेक्षण रिपोर्ट उपलब्ध हो सके.

v. सूचना प्रणाली अंकेक्षण रिपोर्ट उच्च प्रबंधन/ निदेशक मंडल की लेखापरीक्षा समिति/ निदेशक मंडल के समक्ष प्रस्तुत की जानी चाहिए और लेखापरीक्षा नीति में निर्धारित समय सीमा के भीतर अनुपालना सुनिश्चित की जानी चाहिए.

6. इस परिपत्र को अपने बैंक के निदेशक मंडल और लेखापरीक्षा समिति के समक्ष प्रस्तुत किया जाए और यह सुनिश्चित करें कि दिशानिर्देशों का कार्यान्वयन स्थानीय परिस्थितियों और आपके बैंक में कम्प्यूटरीकरण के स्तर के लिए उपयुक्त संशोधनों के साथ कार्यान्वित किया जाता है.

7. कृपया इस परिपत्र की प्राप्ति सूचना हमारे क्षेत्रीय कार्यालय को दें और पुष्टि करें कि आपके बैंक में सूचना प्रणाली अंकेक्षण शुरू हो गई है.

भवदीय

के आर राव

(के आर राव)
मुख्य महाप्रबंधक

संलग्नकः यथोक्त (31 शीटें)

***Annexure-A***

**Broad guidelines for Information System (IS) Audit**

Information System Audit is a series of tests that must be conducted periodically or for special purpose to ensure that adequate controls are in place over the Information System. Information System Audit is not a Financial Statement Audit and it does not test financial statement data for determining existence, completeness, rights and obligations, valuation or allocation and presentation and disclosure.

1. The purpose of IS Audit is to review and provide feedback, assurance and suggestions on the concerns of the management with regard to integrity and effectiveness of systems and control. These concerns can be grouped under three areas which are related to the systems :

1.1 **Availability**: Will the information systems on which the business is heavily dependent be available for the business at all times when required ? Are the systems well protected against all types of losses and disasters? High availability systems aim to remain available at all times preventing service disruptions due to power outage, hardware failures and system upgrades.

1.2 **Confidentiality** : Will the information in the systems be disclosed only to those who is authorized to see and use it and not to anyone else ?

1.3 **Integrity** : Will the information provided by the system always be accurate, reliable and timely? What measures are available to ensure that no unauthorized modification can be made to the data or the software in the system ?

The IS audit aims to provide reasonable assurances on test basis regarding the adequacy of the controls used in the governance over IS resources and covers all the major and common types of audit, viz. Systems Audit, Application audits, Compliance audits, Security audits, Performance audits, etc.

2. Banks which have partially / fully computerized their operations and migrated on CBS system should put in place a mechanism for conducting IS audit on perpetual basis. IS audit should be conducted by a qualified auditor/ audit firm. Banks which have an independent Inspection & Audit Department should constitute an IS audit cell as part of their Inspection and Audit Department to carry out IS audit in branches / offices having computerised operations. However, those banks, which do not have an independent Inspection & Audit Department, should create a dedicated group of persons, who, when required, can perform functions of an IS Auditor. The overall control and supervision of these IS Audit Cells should be vested in the Audit Committees.

3. A team of competent and motivated IS personnel may be developed. It is beneficial to have a collective development system consisting of many persons instead of a few, in order to take care of a possible exodus of key personnel. IS auditors' technical knowledge should be augmented on a continuing basis through their deputation to seminars / conferences, supply of technical periodicals and books etc.

4. Duties of system programmer / designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming / design. System person would only make modifications / improvements to programs and the operating persons would only use such programs without having the right to make any modifications.

5. Major factors which lead to security violations in computers include inadequate or incomplete system design, programming errors, weak or inadequate logical access controls, absent or poorly designed procedural controls, ineffective employee supervision and management controls. These loopholes may be plugged by : (i) strengthening physical, logical and procedural access to system; (ii) introducing standards for quality assurance and periodically testing and checking them; and (iii) screening employees prior to induction into IS application areas and keeping a watch on their behavioral pattern.

6. There is a need for formal declaration of system development methodology, programming and documentation standards to be followed by the bank, in the absence of which quality of system maintenance / improvement might suffer. IS auditors should verify compliance in this regard.

7. Contingency plans / procedures in case of failure of system should be introduced / tested at periodic intervals. IS auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.

8. Every bank should have a manual of instructions for their inspectors / auditors and it should be updated periodically to keep in tune with latest developments in its area of operations and in its policies and procedures.

9. An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements. Before introducing an IS application in place of certain manual procedures, parallel run of both the systems should be done for a reasonable period to ensure that all aspects of security, reliability and accessibility of data are ensured in the IS application.

10. In order to ensure that the IS applications have resulted in a consistent and reliable system for inputting of data, processing and generation of output, various tests to identify erroneous processing, to assess the quality of data, to identify inconsistent data and to compare data with physical forms should be introduced.

11. While engaging outside computer agencies, banks should ensure to incorporate the "clause of visitorial rights" in the contract, so as to have the right to inspect the process of application and also ensure the security of the data / Data Centre / Disaster Recovery Centre / inputs given to such outside agencies. Agreement with vendor should take care of probable data leakage.

12. Entire domain of IS activities (from policy to implementation) should be brought under scrutiny of Inspection and Audit Department. Financial outlay as well as activities to be performed by IS department should be reviewed by senior management at periodic intervals.

13. The information systems auditor is to provide a report in an appropriate form, upon completion of audit work. The audit report is to state the scope, objectives, period of coverage and the nature and extent of the audit work performed. The report is to state the findings, conclusions and recommendations with respect to improvement in data integrity, system effectiveness and system efficiency.

---

# सूचना प्रौद्योगिकी अधिनियम, 2000

(2000 का अधिनियम संख्यांक 21)

[9 जून, 2000]

इलैक्ट्रानिक डाटा के आदान-प्रदान द्वारा और इलैक्ट्रानिक संसूचना के अन्य साधनों द्वारा, जिन्हें सामान्यतया "इलैक्ट्रानिक वाणिज्य" कहा जाता है और जिनमें संसूचना और सूचना के भंडारण के कागज-आधारित तरीकों के अनुकल्पों का उपयोग अंतर्वलित है, किए गए संव्यवहारों को विधिक मान्यता देने, सरकारी अभिकरणों में दस्तावेजों को इलैक्ट्रानिक रूप से फाइल करना सुकर बनाने और भारतीय दंड संहिता, भारतीय साक्ष्य अधिनियम, 1872, बैंककार बही साक्ष्य अधिनियम, 1891 और भारतीय रिजर्व बैंक अधिनियम, 1934 का और संशोधन करने तथा उससे संबंधित या उसके आनुषंगिक विषयों का उपबंध करने के लिए अधिनियम

**नोट:- इस डॉक्यूमेंट में साइबर अपराधों एवं हैकिंग से सम्बंधित महत्त्वपूर्ण धाराओं** (43, 43**ए**, 66, 66**बी**, 66 **सी**, 66**डी**, 66**ई**, 66**एफ**, 67, 67**ए**, 67**बी**, 70, 72, 72**ए तथा** 74) **को ही रखा गया है। अधिनिमय की पूर्ण सॉफ्टकॉपी अपैक्स बैंक वेबसाइट पर देखी जा सकती है।**

**42. प्राइवेट कुंजी का नियंत्रण**—(1) प्रत्येक उपयोगकर्ता, अपने अंकीय चिह्नक प्रमाणपत्र में सूचीबद्ध लोक कुंजी के अनुरूप प्राइवेट कुंजी का नियंत्रण रखने में युक्तियुक्त सावधानी बरतेगा और [1]* * *

(2) यदि अंकीय चिह्नक प्रमाणपत्र में सूचीबद्ध लोक कुंजी के अनुरूप प्राइवेट कुंजी गोपनीय नहीं रह गई है, तो उपयोगकर्ता, इसकी संसूचना प्रमाणकर्ता प्राधिकारी को ऐसी रीति में अविलम्ब देगा, जो विनियमों द्वारा विनिर्दिष्ट की जाए ।

**स्पष्टीकरण**—शंकाओं को दूर करने के लिए यह घोषित किया जाता है कि उपयोगकर्ता तब तक दायी होगा जब तक कि उसने प्रमाणकर्ता प्राधिकारी को सूचित न कर दिया हो कि प्राइवेट कुंजी गोपनीय नहीं रह गई है ।

**अध्याय 9**

## [2][शास्तियां, प्रतिकर और अधिनिर्णय]

**43. कंप्यूटर, कंप्यूटर प्रणाली आदि को नुकसान के लिए** [3][**शास्ति और प्रतिकर**]—यदि कोई व्यक्ति, ऐसे स्वामी या किसी अन्य व्यक्ति की, जो किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क प्रणाली का भारसाधक है, अनुज्ञा के बिना,—

(क) ऐसे कंप्यूटर, कंप्यूटर नेटवर्क [4][या कंप्यूटर संसाधन] प्रणाली में पहुंचता है या पहुंच प्राप्त करता है;

(ख) ऐसे कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क से कोई डाटा, कंप्यूटर डाटा संचय या सूचना, जिसके अंतर्गत किसी स्थानांतरणीय भंडारण माध्यम में धृत या संचित कोई सूचना या डाटा भी हैं, डाउनलोड करता है, प्रतिलिपि करता है, या उसका उद्धरण लेता है;

(ग) किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में किसी कंप्यूटर संदूषक या कंप्यूटर वाइरस का प्रवेश करता है, या प्रवेश करवाता है;

(घ) ऐसे कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में के किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क, डाटा, कंप्यूटर डाटा संचय या किसी अन्य कार्यक्रम को नुकसान पहुंचाता है या पहुंचवाता है;

(ङ) किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क को विच्छिन्न करता है या करवाता है;

(च) किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में पहुंच के लिए प्राधिकृत किसी व्यक्ति की किसी भी साधन से पहुंच से इंकार करता है या करवाता है;

(छ) इस अधिनियम, इसके अधीन बनाए गए नियमों या विनियमों के उल्लंघन में, किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में किसी व्यक्ति की पहुंच को सुकर बनाने के लिए कोई सहायता प्रदान करता है;

(ज) किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में छेड़छाड़ या छलसाधन करके, किसी व्यक्ति द्वारा उपभोग की गई सेवाओं के प्रभारों को किसी अन्य व्यक्ति के लेखे में डालता है,

तो वह इस प्रकार प्रभावित व्यक्ति को प्रतिकर के रूप में ऐसी नुकसानी का जो एक करोड़ रुपए से अधिक नहीं होगी, संदाय करने का दायी होगा ।

[4][(झ) किसी कंप्यूटर संसाधन में विद्यमान किसी सूचना को नष्ट करता है, हटाता है या उसमें परिवर्तन करता है या उसके महत्व या उपयोगिता को कम करता है या उसे किन्हीं साधनों द्वारा हानिकर रूप से प्रभावित करता है;

(ञ) किसी कंप्यूटर संसाधन के लिए प्रयुक्त किसी कंप्यूटर स्रोत कोड को नुकसान पंहुचाने के आशय से चुराता है, छिपाता है, नष्ट या परिवर्तित करता है या किसी व्यक्ति से उसकी चोरी कराता है या उसे छिपवाता, नष्ट या परिवर्तित कराता है,]

[3][तो वह इस प्रकार प्रभावित व्यक्ति को प्रतिकर के रूप में नुकसानी का संदाय करने का दायी होगा;]

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए,—

(i) "कंप्यूटर संदूषक" से कंप्यूटर अनुदेशों का कोई ऐसा सेट अभिप्रेत है, जो निम्नलिखित के लिए अभिकल्पित किया गया हो,—

(क) किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में के डाटा या कार्यक्रम को उपांतरित, नष्ट, अभिलिखित या पारेषित करने; या

---

[1] का० आ० 1015 (अ), तारीख 19-9-2002 द्वारा लोप किया गया ।

[2] 2009 के अधिनियम सं० 10 की धारा 20 द्वारा प्रतिस्थापित ।

[3] 2009 के अधिनियम सं० 10 की धारा 21 द्वारा प्रतिस्थापित ।

[4] 2009 के अधिनियम सं० 10 की धारा 21 द्वारा अंत:स्थापित ।

(ख) कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क के सामान्य प्रवर्तन का किसी भी साधन से अनधिकार ग्रहण करने,

(ii) "कंप्यूटर डाटा संचय" से पाठ, प्रतिबिंब, श्रव्य, दृश्य में सूचना, जानकारी, तथ्य, संकल्पना और अनुदेशों का व्यपदेशन अभिप्रेत है, जो प्रारूपित रीति में तैयार किया जा रहा है या तैयार किया गया है अथवा कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क द्वारा उत्पादित किया गया है और जो कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क में उपयोग के लिए आशयित है;

(iii) कंप्यूटर वाइरस से ऐसा कोई कंप्यूटर अनुदेश, सूचना, डाटा या कार्यक्रम अभिप्रेत है जो किसी कंप्यूटर साधन के निष्पादन को नष्ट करता है, नुकसान पहुंचाता है, ह्रास करता है या प्रतिकूल प्रभाव डालता है अथवा स्वयं को किसी अन्य कंप्यूटर साधन से संलग्न कर लेता है और वह तब प्रवर्तित होता है जब कोई कार्यक्रम, डाटा या अनुदेश निष्पादित किया जाता है या उस कंप्यूटर साधन में कोई अन्य घटना घटती है;

(iv) "नुकसान" से किसी माध्यम द्वारा किसी कंप्यूटर साधन को नष्ट करना, परिवर्तित करना, हटाना, जोड़ना, उपान्तरित या पुन: व्यवस्थित करना अभिप्रेत है;

[1][(v) "कंप्यूटर स्रोत कोड" से कंप्यूटर संसाधन के कार्यक्रमों, कंप्यूटरों समादेशों, डिजाइन और रेखांक तथा कार्यक्रम विश्लेषण को किसी रूप में सूचीबद्ध करना अभिप्रेत है ।]

[2][**43क. डाटा को संरक्षित रखने में असफलता के लिए प्रतिकर**—जहां कोई निगमित निकाय ऐसे किसी कंप्यूटर संसाधन में किसी संवेदनशील व्यक्तिगत डाटा या सूचना को रखता है, उसका संव्यवहार करता है या उसको संभालता है जो उसके स्वामित्व में, नियंत्रण में है या जिसका वह प्रचालन करता है, युक्तियुक्त सुरक्षा पद्धतियों और प्रक्रियाओं के कार्यान्वयन और अनुरक्षण में उपेक्षा करता है और उसके द्वारा किसी व्यक्ति को सदोष हानि या सदोष लाभ पहुंचाता है, वहां ऐसा निगमित निकाय, इस प्रकार प्रभावित व्यक्ति को प्रतिकर के रूप में नुकसानी का संदाय करने के लिए दायी होगा ।

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए,—

(i) "निगमित निकाय" से कोई कंपनी अभिप्रेत है और इसके अंतर्गत वाणिज्यिक या वृत्तिक क्रियाकलापों में लगी हुई फर्म, एकल स्वामित्व या व्यष्टियों का कोई अन्य संगम भी है;

(ii) "युक्तियुक्त सुरक्षा पद्धतियों और प्रक्रियाओं" से ऐसी अप्राधिकृत पहुंच, नुकसानी, उपयोग, उपांतरण, प्रकटन या ह्रास, जो, यथास्थिति, पक्षकारों के बीच किसी करार में विनिर्दिष्ट किया जाए या जो तत्समय प्रवृत्त किसी विधि में विनिर्दिष्ट किया जाए ऐसी सूचना को संरक्षित करने के लिए अभिकल्पित सुरक्षा पद्धतियों और प्रक्रियाएं और ऐसे करार या किसी विधि के अभाव में, ऐसी युक्तियुक्त सुरक्षा पद्धतियां और प्रक्रियाएं, जो केन्द्रीय सरकार द्वारा ऐसे वृत्तिक निकायों या संगमों के परामर्श से, जिन्हें वह उपयुक्त समझे, विहित की जाएं, अभिप्रेत हैं;

(iii) "संवेदनशील व्यक्तिगत डाटा या सूचना" से ऐसी व्यक्तिगत सूचना अभिप्रेत है जो केन्द्रीय सरकार द्वारा ऐसे वृत्तिक निकायों या संगमों के परामर्श से, जिन्हें वह उचित समझे, विहित की जाए ।]

**44. जानकारी, विवरणी, आदि देने में असफल रहने के लिए शास्ति**—यदि कोई ऐसा व्यक्ति, जिससे इस अधिनियम या इसके अधीन बनाए गए किन्हीं नियमों या विनियमों के अधीन,—

(क) नियंत्रक अथवा प्रमाणकर्ता प्राधिकारी को कोई दस्तावेज, विवरणी या रिपोर्ट देना अपेक्षित है, उसे देने में असफल रहेगा, तो वह, ऐसी प्रत्येक असफलता के लिए एक लाख पचास हजार रुपए से अनधिक की शास्ति का दायी होगा;

(ख) विनियमों में उनके देने के लिए विनिर्दिष्ट समय के भीतर कोई विवरणी फाइल करने या कोई जानकारी, पुस्तक या अन्य दस्तावेज देना अपेक्षित है, विनियमों में उनके देने के लिए विनिर्दिष्ट समय के भीतर विवरणी फाइल करने या उसे देने में असफल रहेगा, तो वह, ऐसे प्रत्येक दिन के लिए, जिसके दौरान ऐसी असफलता बनी रहती है, पाचं हजार रुपए से अनधिक की शास्ति का दायी होगा;

(ग) लेखा बहियां या अभिलेख बनाए रखना अपेक्षित है, उन्हें बनाए रखने में असफल रहता है, तो वह, ऐसे प्रत्येक दिन के लिए, जिसके दौरान ऐसी असफलता बनी रहती है, दस हजार रुपए से अनधिक की शास्ति का दायी होगा ।

**45. अवशिष्ट शास्ति**—जो कोई, इस अधिनियम के अधीन बनाए गए किन्हीं नियमों या विनियमों का उल्लंघन करेगा, तो वह ऐसे उल्लंघन के लिए, जिसके लिए अलग से किसी शास्ति का उपबंध नहीं किया गया है, ऐसे उल्लंघन से प्रभावित व्यक्ति को पच्चीस हजार रुपए से अनधिक के प्रतिकर का संदाय करने या पच्चीस हजार रुपए से अनधिक की शास्ति का दायी होगा ।

---

[1] 2009 के अधिनियम सं० 10 की धारा 21 द्वारा अंत:स्थापित ।

[2] 2009 के अधिनियम सं० 10 की धारा 21 द्वारा प्रतिस्थापित ।

परन्तु यदि उच्च न्यायालय का यह समाधान हो जाता है कि अपीलार्थी, उक्त अवधि के भीतर अपील फाइल करने से पर्याप्त कारण से निवारित किया गया था तो वह ऐसी और अवधि के भीतर, जो साठ दिन से अधिक नहीं होगी, अपील फाइल करने के लिए अनुज्ञात कर सकेगा ।

**63. अपराधों का शमन**—(1) इस [1][अधिनियम] के अधीन कोई उल्लंघन, न्यायनिर्णयन कार्यवाहियों के संस्थापन के पूर्व या पश्चात्, यथास्थिति, नियंत्रक या उसके द्वारा इस निमित्त विशेष रूप से प्राधिकृत किसी अन्य अधिकारी द्वारा या न्यायनिर्णायक अधिकारी द्वारा, ऐसी शर्तों के अधीन रहते हुए, जो नियंत्रक या ऐसे अन्य अधिकारी द्वारा विनिर्दिष्ट की जाए, शमन किया जा सकेगा :

परन्तु ऐसी राशि, किसी भी दशा में, शास्ति की उस अधिकतम रकम से अधिक नहीं होगी, जो इस अधिनियम के अधीन इस प्रकार शमन किए गए उल्लंघन के लिए अधिरोपित है ।

(2) उपधारा (1) की कोई बात, उस व्यक्ति को लागू नहीं होगी, जो उसके द्वारा किए गए पहले उल्लंघन, जिसका शमन किया गया था, की तारीख से तीन वर्ष की अवधि के भीतर वही या वैसा ही उल्लंघन करता है ।

**स्पष्टीकरण**—इस उपधारा के प्रयोजनों के लिए, उस तारीख से, जिसको उल्लंघन का पहले शमन किया गया था, तीन वर्ष की अवधि की समाप्ति के पश्चात् किया गया कोई दूसरा या पश्चात्वर्ती उल्लंघन पहला उल्लंघन समझा जाएगा ।

(3) जहां उपधारा (1) के अधीन किसी उल्लंघन का शमन किया गया है, वहां इस प्रकार शमन किए गए उल्लंघन की बाबत उस उल्लंघन के दोषी व्यक्ति के विरुद्ध, यथास्थिति, कोई कार्यवाही या अतिरिक्त कार्यवाही नहीं की जाएगी ।

**64. [2][शास्ति या प्रतिकर की वसूली]**—इस अधिनियम के अधीन [2][अधिरोपित शास्ति, या अधिनिर्णीत प्रतिकर] यदि उसका संदाय नहीं किया जाता है, भू-राजस्व की बकाया के रूप में वसूल की जाएगी और, यथास्थिति, अनुज्ञप्ति या [3][इलैक्ट्रानिक चिह्नक] प्रमाणपत्र शास्ति का संदाय किए जाने तक निलंबित रखा जाएगा ।

**अध्याय 11**

## अपराध

**65. कंप्यूटर साधन कोड से छेड़छाड़**—जो कोई, कम्प्यूटर, कम्प्यूटर कार्यक्रम, कम्प्यूटर प्रणाली या कम्प्यूटर नेटवर्क के लिए उपयोग किए जाने वाले किसी कम्प्यूटर साधन कोड को, जब कम्प्यूटर साधन कोड का रखा जाना या अनुरक्षित किया जाना तत्समय प्रवृत्त विधि द्वारा अपेक्षित हो, जानबूझकर या साशय छिपाता है, नष्ट करता है या परिवर्तित करता है अथवा साशय या जानबूझकर किसी अन्य से छिपवाता है, नष्ट कराता है या परिवर्तित कराता है तो वह कारावास से, जो तीन वर्ष तक का हो सकेगा या जुर्माने से, जो दो लाख रुपए तक का हो सकेगा, या दोनों से, दंडनीय होगा ।

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए, "कम्प्यूटर साधन कोड" से कार्यक्रमों, कम्प्यूटर समादेशों, डिजाइन और विन्यास का सूचीबद्ध करना तथा कम्प्यूटर साधन का किसी भी रूप में कार्यक्रम विश्लेषण अभिप्रेत है ।

[4][**66. कंप्यूटर से संबंधित अपराध**—यदि कोई व्यक्ति, धारा 43 में निर्दिष्ट कोई कार्य बेईमानी से या कपटपूर्वक करता है तो वह कारावास से, जिसकी अवधि तीन वर्ष तक की हो सकेगी या जुर्माने से, जो पांच लाख रुपए तक का हो सकेगा या दोनों से, दंडनीय होगा ।

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए,—

(क) "बेईमानी से" शब्दों का वही अर्थ है जो भारतीय दंड संहिता (1860 का 45) की धारा 24 में है;

(ख) "कपटपूर्वक" शब्द का वही अर्थ है जो भारतीय दंड संहिता (1860 का 45) की धारा 25 में है ।

**66क. संसूचना सेवा आदि द्वारा आक्रामक संदेश भेजने के लिए दंड**—कोई व्यक्ति, जो किसी कंप्यूटर संसाधन या किसी संसूचना के माध्यम से,—

(क) ऐसी किसी सूचना को, जो अत्यधिक आक्रामक या धमकाने वाली प्रकृति की है; या

(ख) ऐसी किसी सूचना को, जिसका वह मिथ्या होना जानता है, किंतु क्षोभ, असुविधा, खतरा, रुकावट, अपमान, क्षति या आपराधिक अभित्रास, शत्रुता, घृणा या वैमनस्य फैलाने के प्रयोजन के लिए, लगातार ऐसे कंप्यूटर संसाधन या किसी संसूचना युक्ति का उपयोग करके,

---

[1] का० आ० 1015 (अ), तारीख 19-9-2002 द्वारा प्रतिस्थापित ।

[2] 2009 के अधिनियम सं० 10 की धारा 31 द्वारा प्रतिस्थापित ।

[3] 2009 के अधिनियम सं० 10 की धारा 2 द्वारा प्रतिस्थापित ।

[4] 2009 के अधिनियम सं० 10 की धारा 32 द्वारा प्रतिस्थापित ।

(ग) ऐसी किसी इलैक्ट्रानिक डाक या इलैक्ट्रानिक डाक संदेश को, ऐसे संदेशों के उद्गम के बारे में प्रेषिती या पाने वाले को क्षोभ या असुविधा कारित करने या प्रवंचित या भ्रमित करने के प्रयोजन के लिए,

भेजता है तो वह ऐसे कारावास से, जिसकी अवधि तीन वर्ष तक की हो सकेगी और जुर्माने से, दंडनीय होगा ।

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए, "इलैक्ट्रानिक डाक" और "इलैक्ट्रानिक डाक संदेश" पदों से किसी कंप्यूटर, कंप्यूटर प्रणाली, कंप्यूटर संसाधन या संचार युक्ति में सृजित या पारेषित या प्राप्त किया गया कोई संदेश या सूचना अभिप्रेत है, जिसके अंतर्गत पाठ, आकृति, आडियो, वीडियो और किसी अन्य इलैक्ट्रानिक अभिलेख के ऐसे संलग्नक भी है, जो संदेश के साथ भेजे जाएं ।

**66ख. चुराए गए कंप्यूटर संसाधन या संचार युक्ति को बेइमानी से प्राप्त करने के लिए दंड**—जो कोई ऐसे किसी चुराए गए कंप्यूटर संसाधन या संचार युक्ति को, जिसके बारे में वह यह जानता है या उसके पास यह विश्वास करने का कारण है कि वह चुराया गया कंप्यूटर संसाधन या संचार युक्ति है, बेईमानी से प्राप्त करेगा या प्रतिधारण करेगा, तो वह दोनों में से किसी भी भांति के कारावास से, जिसकी अवधि तीन वर्ष तक की हो सकेगी या जुर्माने से, जो एक लाख रुपए तक का हो सकेगा, या दोनों से, दंडित किया जाएगा ।

**66ग. पहचान चोरी के लिए दंड**—जो कोई कपटपूर्वक या बेईमानी से किसी अन्य व्यक्ति के इलैक्ट्रानिक चिह्नक, पासवर्ड या किसी अन्य विशिष्ट पहचान चिह्न का प्रयोग करेगा, तो वह दोनों में से किसी भी भांति के कारावास से, जिसकी अवधि तीन वर्ष तक की हो सकेगी, दंडित किया जाएगा और जुर्माने के लिए भी, जो एक लाख रुपए तक का हो सकेगा, दायी होगा ।

**66घ. कंप्यूटर संसाधन का उपयोग करके प्रतिरूपण द्वारा छल करने के लिए दंड**—जो कोई, किसी संचार युक्ति या कंप्यूटर संसाधन के माध्यम से प्रतिरूपण द्वारा छल करेगा, तो वह दोनों में से किसी भी भांति के कारावास से, जिसकी अवधि तीन वर्ष तक की हो सकेगी, दंडित किया जाएगा और जुर्माने के लिए भी, जो एक लाख रुपए तक का हो सकेगा, दायी होगा ।

**66ङ. एकांतता के अतिक्रमण के लिए दंड**—जो कोई, साशय या जानबूझकर किसी व्यक्ति के गुप्तांग के चित्र उसकी सहमति के बिना उस व्यक्ति की एकांतता का अतिक्रमण करने वाली परिस्थितियों में खींचेगा, प्रकाशित या पारेषित करेगा, वह ऐसे कारावास से, जो तीन वर्ष तक का हो सकेगा या जुर्माने से, जो दो लाख रुपए से अधिक का नहीं हो सकेगा या दोनों से, दंडित किया जाएगा ।

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए,—

(क) "पारेषण" से किसी दृश्यमान चित्र को इस आशय से इलैक्ट्रानिक रूप में भेजना अभिप्रेत है कि उसे किसी व्यक्ति या व्यक्तियों द्वारा देखा जाए;

(ख) किसी चित्र के संबंध में "चित्र खींचना" से वीडियो टेप, फोटोग्राफ, फिल्म तैयार करना या किसी साधन द्वारा अभिलेख बनाना अभिप्रेत है;

(ग) "गुप्तांग" से नग्न या अंत:वस्त्र सज्जित जननांग, जघन अंग, नितंब या स्त्री स्तन अभिप्रेत हैं;

(घ) "प्रकाशित करने" से मुद्रित या इलैक्ट्रानिक रूप में पुन:निर्माण करना और उसे जनसाधारण के लिए उपलब्ध कराना अभिप्रेत है;

(ङ) "एकांतता का अतिक्रमण करने वाली परिस्थितियों के अधीन" से ऐसी परिस्थितियां अभिप्रेत हैं, जिनमें किसी व्यक्ति को यह युक्तियुक्त प्रत्याशा हो सकती है कि,—

(i) वह इस बात की चिंता किए बिना कि उसके गुप्तांग का चित्र खींचा जा रहा है; एकांतता में अपने वस्त्र उतार सकता या उतार सकती है, या

(ii) इस बात पर ध्यान दिए बिना कि वह व्यक्ति किसी सार्वजनिक स्थान या निजी स्थान में है उसके गुप्तांग का कोई भाग जनसाधारण को दृश्यमान नहीं होगा ।

**66च. साइबर आतंकवाद के लिए दंड**—(1) जो कोई,—

(अ) भारत की एकता, अखंडता, सुरक्षा या प्रभुता को खतरे में डालने या जनता या जनता के किसी वर्ग में,—

(i) कंप्यूटर संसाधन तक पहुंच के लिए प्राधिकृत किसी व्यक्ति को पहुंचे से इंकार करके या इंकार कराके; या

(ii) प्राधिकार के बिना या प्राधिकृत पहुंच से अधिक किसी कंप्यूटर संसाधन में प्रवेश या उस तक पहुंच करने का प्रयास करके; या

(iii) किसी कंप्यूटर संदूषक को सन्निविष्ट करके या सन्निविष्ट कराके,

आतंक फैलाने के आशय से और ऐसा करके ऐसा कार्य करता है जिससे व्यक्तियों की मृत्यु या उन्हें क्षति होती है या संपत्ति का नाशा या विनाश होता है या होने की संभावना है या यह जानते हुए कि इससे समुदाय के जीवन के लिए आवश्यक आपूर्ति या

सेवाओं को नुकसान या उसका विनाश होने की संभावना है या धारा 70 के अधीन विनिर्दिष्ट संवेदनशील सूचना अवसंरचना पर प्रतिकूल प्रभाव पड़ने की संभावना है; या

(आ) जानबूझकर या साशय किसी कंप्यूटर संसाधन में प्राधिकार के बिना या प्राधिकृत पहुंच से अधिक प्रवेश या पहुंच करता है और ऐसे कार्य द्वारा ऐसी सूचना, डाटा या कंप्यूटर डाटा आधारसामग्री तक, जो राष्ट्रीय सुरक्षा या विदेशी संबंधों के कारण निर्बंधित है या कोई निर्बंधित सूचना डाटा या कंप्यूटर डाटा आधारसामग्री तक यह विश्वास करते हुए पहुंच प्राप्त करता है कि इस प्रकार अभिप्राप्त ऐसी सूचना, डाटा या कंप्यूटर डाटा आधारसामग्री का उपयोग भारत की प्रभुता और अखण्डता, राज्य की सुरक्षा, विदेशों के साथ मैत्रीपूर्ण संबंधों, लोक व्यवस्था, शिष्टता या नैतिकता के हितों को या न्यायालय की अवमानना के संबंध मे, मानहानि या किसी अपराध के उत्प्रेरण के संबंध में किसी विदेशी राष्ट्र, व्यष्टि, समूह के फायदे को क्षति पहुंचाने के लिए या अन्यथा किया जा सकता है या किए जाने की संभावना है,

तो वह साइबर आतंकवाद का अपराध करेगा ।

(2) जो कोई साइबर आतंकवाद कारित या करने की कूटरचना करेगा, तो वह कारावास से जो आजीवन कारावास तक का हो सकेगा, दंडनीय होगा ।

**67. अश्लील सामग्री का इलैक्ट्रानिक रूप में प्रकाशन या पारेषण करने के लिए दंड**—जो कोई, इलैक्ट्रानिक रूप में, ऐसी सामग्री को प्रकाशित या पारेषित करता है अथवा प्रकाशित या पारेषित कराता है, जो कामोत्तेजक है या जो कामुकता की अपील करती है या यदि इसका प्रभाव ऐसा है जो व्यक्तियों को कलुषित या भ्रष्ट करने का आशय रखती है जिसमें सभी सुसंगत परिस्थितियों को ध्यान में रखते हुए उसमें अंर्तविष्ट या उसमें आरुढ़ सामग्री को पढ़ने, देखने या सुनने की संभावना है, पहली दोषसिद्धि पर, दोनों में से किसी भी भांति के कारावास से, जिसकी अवधि तीन वर्ष तक की हो सकेगी और जुर्माने से, जो पांच लाख रुपए तक का हो सकेगा, और दूसरी या पश्चात्वर्ती दोषसिद्धि की दशा में, दोनों में से किसी भी भांति के कारावास से, जिसकी अवधि पांच वर्ष तक की हो सकेगी और जुर्माने से भी, जो दस लाख रुपए तक का हो सकेगा, दंडित किया जाएगा ।

**67क. कामुकता व्यक्त करने वाले कार्य आदि वाली सामग्री के इलैक्ट्रानिक रूप में प्रकाशन के लिए दंड**—जो कोई, किसी ऐसी सामग्री को इलैक्ट्रानिक रूप में प्रकाशित करता है या पारेषित करता है या प्रकाशित या पारेषित कराता है, जिसमें कामुकता व्यक्त करने का कार्य या आचरण अंतर्वलित है, पहली दोषसिद्धि पर, दोनों में से किसी भी भांति के कारावास से, जिसकी अवधि पांच वर्ष तक की हो सकेगी और जुर्माने से, जो दस लाख रुपए तक का हो सकेगा और दूसरी या पश्चात्वर्ती दोषसिद्धि की दशा में, दोनों में से किसी भी भांति के कारावास से, जिसकी अवधि सात वर्ष तक की हो सकेगी और जुर्माने से भी, जो दस लाख रुपए तक का हो सकेगा, दंडित किया जाएगा ।

**67ख. कामुकता व्यक्त करने वाले कार्य आदि में बालकों को चित्रित करने वाली सामग्री को इलैक्ट्रानिक रूप में प्रकाशित या पारेषित करने के लिए दंड**—जो कोई,—

(क) किसी इलैक्ट्रानिक रूप में ऐसी कोई सामग्री प्रकाशित या पारेषित करेगा या प्रकाशित या पारेषित कराएगा, जिसमें कामुकता व्यक्त करने वाले कार्य या आचरण में लगाए गए बालकों को चित्रित किया जाता है; या

(ख) अश्लील या अभद्र या कामुकता व्यक्त करने वाली रीति में बालकों का चित्रण करने वाली सामग्री का पाठ या अंकीय चित्र किसी इलैक्ट्रानिक रूप में तैयार करेगा, संगृहीत करेगा, प्राप्त करेगा, पढ़ेगा, डाउनलोड करेगा, उसे बढ़ावा देगा, आदान-प्रदान या वितरित करेगा; या

(ग) कामुकता व्यक्त करने वाले कार्य के लिए और उसके संबंध में या ऐसी रीति में बालकों को एक या अधिक बालकों के साथ आन-लाइन संबंध के लिए लगाएगा, फुसलाएगा या उत्प्रेरित करेगा, जो कंम्पयूटर संसाधन पर किसी युक्तियुक्त वयस्क को बुरी लग सकती है; या

(घ) आन-लाइन बालकों का दुरुपयोग किए जाने को सुकर बनाएगा; या

(ङ) बालकों के साथ कामुकता व्यक्त करने वाले कार्य के संबंध में अपने दुर्व्यवहार को किसी इलैक्ट्रानिक रूप में अभिलिखित करेगा,

तो वह प्रथम दोषसिद्धि पर दोनों में से किसी भांति के कारावास से, जिसकी अवधि पांच वर्ष तक की हो सकेगी और जुर्माने से, जो दस लाख रुपए तक का हो सकेगा, और दूसरी और पश्चात्वर्ती दोषसिद्धि पर दोनों में से किसी भांति के कारावास से, जिसकी अवधि सात वर्ष तक की हो सकेगी और जुर्माने से भी, जो दस लाख रुपए तक का हो सकेगा, दंडित किया जाएगा :

परन्तु धारा 67, धारा 67क और इस धारा के उपबंधों का विस्तार निम्नलिखित किसी पुस्तक, पर्चे, पत्र, लेख, रेखाचित्र, पेंटिंग, प्रदर्शन या इलैक्ट्रानिक रूप में आकृति पर नहीं है :—

(i) जिसका प्रकाशन इस आधार पर जनकल्याण के रूप में न्यायोचित साबित किया गया हो कि ऐसी पुस्तक, पर्चे, पत्र, लेख, रेखाचित्र, पेंटिंग, प्रदर्शन या आकृति, विज्ञान, साहित्य या शिक्षण या सामान्य महत्व के अन्य उद्देश्यों के हित में है; या

(ii) जो सद्भाविक परंपरा या धार्मिक प्रयोजनों के लिए रखी या प्रयुक्त की गई है ।

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए, "बालक" से ऐसा व्यक्ति अभिप्रेत है जिसने अठारह वर्ष की आयु पूरी नहीं की है ।

**67ग. मध्यवर्तियों द्वारा सूचना का परिरक्षण और प्रतिधारण**—(1) मध्यवर्ती ऐसी सूचना का, जो विनिर्दिष्ट की जाए, परिरक्षण और प्रतिधारण ऐसी अवधि के लिए और ऐसी रीति तथा रूप में करेगा जो केन्द्रीय सरकार विहित करे ।

(2) ऐसा कोई मध्यवर्ती, जो साशय या जानबूझकर उपधारा (1) के उपबंधों का उल्लंघन करता है, कारावास, जिसकी अवधि तीन वर्ष तक की हो सकेगी, दंडनीय होगा और जुर्माने का भी दायी होगा ।]

**68. नियंत्रक की निदेश देने की शक्ति**—(1) नियंत्रक, आदेश द्वारा, प्रमाणकर्ता प्राधिकारी या ऐसे प्राधिकारी के किसी कर्मचारी को आदेश में विनिर्दिष्ट उपाय करने या ऐसे क्रियाकलापों को बंद कर देने का निदेश दे सकेगा यदि वे इस अधिनियम या इसके अधीन बनाए गए नियमों या किन्हीं विनियमों के किन्हीं उपबंधों के अनुपालन को सुनिश्चित करने के लिए आवश्यक हैं ।

[1][(2) कोई व्यक्ति, जो उपधारा (1) के अधीन किसी आदेश का अनुपालन करने में साशय या जानबूझकर असफल रहता है, अपराध का दोषी होगा और दोषसिद्धि पर कारावास का, जिसकी अवधि दो वर्ष से अधिक की नहीं होगी या एक लाख रुपए से अनधिक के जुर्माने का या दोनों का दायी होगा ।]

[2][**69. किसी कम्प्यूटर संसाधन के माध्यम से किसी सूचना के अन्तररोधन या मानिटरिंग या विगूढन के लिए निदेश जारी करने की शक्ति**—(1) जहां केन्द्रीय सरकार या किसी राज्य सरकार या यथास्थिति, केन्द्रीय सरकार या राज्य सरकार द्वारा इस निमित्त विशेष रूप से प्राधिकृत उसके किसी अधिकारी का यह समाधान हो जाता है कि भारत की प्रभुता या अखंडता, भारत की रक्षा, राज्य की सुरक्षा, विदेशी राज्यों के साथ मैत्रीपूर्ण संबंधों या लोक व्यवस्था के हित में अथवा उपरोक्त से संबंधित किसी संज्ञेय अपराध के किए जाने में उद्दीपन के निवारण या किसी अपराध के अन्वेषण के लिए ऐसा करना आवश्यक और समीचीन है, वहां वह उपधारा (2) के उपबंधों के अधीन रहते हुए, लेखबद्ध किए जाने वाले कारणों से आदेश द्वारा समुचित सरकार के किसी अभिकरण को, किसी कम्प्यूटर संसाधन में जनित, पारेषित, प्राप्त या भण्डारित किसी सूचना को अंतर्रुद्ध या मानीटर करने अथवा विगूढन करने अथवा अंतर्रुद्ध या मानीटर कराने या विगूढ न कराने का निदेश दे सकेगी ।

(2) प्रक्रिया और रक्षोपाय, जिनके अधीन ऐसा अंतररोधन या मानीटरिंग या विगूढन किया जा सकेगा, वे होंगे, जो विहित किए जाएं ।

(3) उपयोगकर्ता या मध्यवर्ती या कम्प्यूटर संसाधन का भारसाधक कोई व्यक्ति, उपधारा (1) में निर्दिष्ट किसी अभिकरण द्वारा मांगे जाने पर, निम्नलिखित के लिए सभी सुविधाएं और तकनीकी सहायता प्रदान करेगा—

(क) ऐसी सूचना जनित करने, पारेषित करने, प्राप्त करने या भंडार करने वाले कम्प्यूटर संसाधन तक पहुंच उपलब्ध कराना या पहुंच सुनिश्चित करना; या

(ख) यथास्थिति, सूचना को अंतर्रुद्ध, मानीटर या विगूढन करना; या

(ग) कम्प्यूटर संसाधन में भंडारित सूचना उपलब्ध कराना ।

(4) ऐसा उपयोगकर्ता या मध्यवर्ती या कोई व्यक्ति जो उपधारा (3) में विनिर्दिष्ट अभिकरण की सहायता करने में असफल रहता है, कारावास से, जिसकी अवधि सात वर्ष तक की हो सकेगी दंडित किया जाएगा और जुर्माने का भी दायी होगा ।

**69क. किसी कम्प्यूटर संसाधन के माध्यम से किसी सूचना की सार्वजनिक पहुंच के अवरोध के लिए निदेश जारी करने की शक्ति**—(1) जहां केन्द्रीय सरकार या इस निमित्त उसके द्वारा विशेष रूप से प्राधिकृत उसके किसी अधिकारी का यह समाधान हो जाता है कि भारत की प्रभुता और अखंडता, भारत की रक्षा, राज्य की सुरक्षा, विदेशी राज्यों के साथ मैत्रीपूर्ण सबंधों या लोक व्यवस्था के हित में या उपरोक्त से संबंधित किसी संज्ञेय अपराध के किए जाने में उद्दीपन को रोकने के लिए ऐसा करना आवश्यक और समीचीन है, वहां वह उपधारा (2) के उपबंधों के अधीन रहते हुए उन कारणों से जो लेखबद्ध किए जाएंगे, आदेश द्वारा सरकार के किसी अभिकरण या मध्यवर्ती को किसी कंप्यूटर संसाधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित किसी सूचना को जनता की पहुंच के लिए अवरुद्ध करने का निदेश दे सकेगा या उसका अवरोध कराएगा ।

(2) वह प्रक्रिया और रक्षोपाय, जिनके अधीन जनता की पहुंच के लिए ऐसा अवरोध किया जा सकेगा, वे होंगे, जो विहित किए जाएं ।

(3) वह मध्यवर्ती जो उपधारा (1) के अधीन जारी निर्देश का पालन करने में असफल रहता है, कारावास से जिसकी अवधि सात वर्ष तक की हो सकेगी, दंडित किया जाएगा और जुर्माने का भी दायी होगा ।

---

[1] 2009 के अधिनियम सं० 10 की धारा 33 द्वारा प्रतिस्थापित ।

[2] 2009 के अधिनियम सं० 10 की धारा 34 द्वारा प्रतिस्थापित ।

**69ख. साइबर सुरक्षा के लिए किसी कम्प्यूटर संसाधन के माध्यम से ट्रैफिक आंकड़ा या सूचना मानीटर करने और एकत्र करने के लिए प्राधिकृत करने की शक्ति**—(1) केन्द्रीय सरकार, देश में साइबर सुरक्षा बढ़ाने और कंप्यूटर संदूषक की पहचान, विश्लेषण और अनाधिकार प्रवेश या फैलाव को रोकने के लिए, राजपत्र में अधिसूचना द्वारा, किसी कंप्यूटर संसाधन में जनित, पारेषित, प्राप्त या भंडारित ट्रैफिक आंकड़ा या सूचना, मानीटर और एकत्र करने के लिए सरकार के किसी अभिकरण को प्राधिकृत कर सकेगी ।

(2) मध्यवर्ती या कम्प्यूटर संसाधन का भारसाधक कोई व्यक्ति, जब ऐसे अभिकरण द्वारा मांग की जाती है, जिसे उपधारा (1) के अधीन प्राधिकृत किया गया है, तकनीकी सहायता उपलब्ध कराएगा और आन-लाइन पहुंच को समर्थ बनाने के लिए ऐसे अभिकरण को सभी सुविधाएं देगा या ऐसे ट्रैफिक आंकड़े या सूचना जनित, पारेषित, प्राप्त या भंडारित करने वाले कम्प्यूटर संसाधन को आन-लाइन पहुंच सुरक्षित कराएगा और उपलब्ध कराएगा ।

(3) ट्रैफिक आंकड़ा या सूचना को मानीटर और एकत्र करने के लिए प्रक्रिया और रक्षोपाय वे होंगे, जो विहित किए जाएं ।

(4) ऐसा कोई मध्यवर्ती जो साशय या जानबूझकर उपधारा (2) के उपबंधों का उल्लंघन करता है कारावास, जिसकी अवधि तीन वर्ष तक की हो सकेगी दंडित किया जाएगा और जुर्माने का भी दायी होगा ।

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए—

(i) "कंप्यूटर संदूषण" का वही अर्थ होगा जो धारा 43 में है;

(ii) "ट्रैफिक आंकड़ा" से ऐसे किसी व्यक्ति, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क या अवस्थिति की पहचान करने वाला या पहचान करने के लिए तात्पर्यित कोई डाटा अभिप्रेत है जिसको या जिससे संसूचना पारेषित की गई या पारेषित की जाए और इसके अंतर्गत संसूचना उद्गम, गंतव्य मार्ग, समय, तारीख, आकार, की गई सेवा की अवधि या प्रकार और कोई अन्य सूचना भी है ।]

**70. संरक्षित प्रणाली**—[1][(1) समुचित सरकार, राजपत्र में अधिसूचना द्वारा, किसी ऐसे कम्प्यूटर संसाधन को, जो प्रत्यक्षत: या अप्रत्यक्षत: नाजुक सूचना अवसंरचना की सुविधा को प्रभावित करता है, सरंक्षित प्रणाली घोषित कर सकेगी ।

**स्पष्टीकरण**—इस धारा के प्रयोजनों के लिए, "नाजुक सूचना अवसंरचना" से ऐसा कंप्यूटर संसाधन अभिप्रेत है, जिसके अक्षमीकरण या नाश से राष्ट्रीय सुरक्षा, अर्थव्यवस्था, लोक स्वास्थ्य या सुरक्षा कमजोर होगी ।]

(2) समुचित सरकार, लिखित आदेश द्वारा, ऐसे व्यक्ति को प्राधिकृत कर सकेगी जो उपधारा (1) के अधीन अधिसूचित संरक्षित प्रणाली तक पहुंचने के लिए प्राधिकृत है ।

(3) कोई व्यक्ति, जो इस धारा के उपबंधों के उल्लंघन में किसी संरक्षित प्रणाली तक पहुंच प्राप्त कर लेता है या पहुंच प्राप्त करने का प्रयत्न करता है, दोनों में से किसी भांति के कारावास से, जिसकी अवधि दस वर्ष तक की हो सकेगी, दंडित किया जाएगा और जुर्माने का भी दायी होगा ।

[2][(4) केन्द्रीय सरकार, ऐसी संरक्षित प्रणाली के लिए सूचना सुरक्षा पद्धतियां और प्रक्रियाएं विहित करेगी ।]

[3]**[70क. राष्ट्रीय नोडल अभिकरण**—(1) केन्द्रीय सरकार, राजपत्र में प्रकाशित अधिसूचना द्वारा, सरकार के किसी संगठन को नाजुक सूचना अवसंरचना संरक्षण की बाबत राष्ट्रीय नोडल अभिकरण अभिहित कर सकेगी ।

(2) उपधारा (1) के अधीन अभिहित राष्ट्रीय नोडल अभिकरण सभी उपायों के लिए उत्तरदायी होगा जिनके अंतर्गत नाजुक सूचना अवसंरचना के संरक्षण से संबंधित अनुसंधान और विकास भी है ।

(3) उपधारा (1) में निर्दिष्ट अभिकरण के कृत्यों और कर्तव्यों के पालन की रीति वह होगी, जो विहित की जाए ।

**70ख. दुर्घटना मोचन के लिए भारतीय कंप्यूटर आपात मोचन दल का राष्ट्रीय आपात अभिकरण के रूप में सेवा करना**—(1) केंद्रीय सरकार, राजपत्र में अधिसूचना द्वारा, सरकार के किसी अभिकरण को नियुक्त करेगा जिसे भारतीय कंप्यूटर आपात मोचन दल कहा जाएगा ।

(2) केंद्रीय सरकार, उपधारा (1) में निर्दिष्ट अभिकरण में एक महानिदेशक और ऐसे अन्य अधिकारी तथा कर्मचारी उपलब्ध कराएगी, जो विहित किए जाएं ।

(3) महानिदेशक और अन्य अधिकारियों तथा कर्मचारियों का वेतन और भत्ते तथा उनकी सेवा के निबंधन और शर्तें वे होंगी, जो विहित की जाएं ।

(4) भारतीय कंप्यूटर आपात मोचन दल साइबर सुरक्षा के क्षेत्र में निम्नलिखित कृत्यों का पालन करने वाले राष्ट्रीय अभिकरण के रूप में कार्य करेगा,—

---

[1] 2009 के अधिनियम सं० 10 की धारा 35 द्वारा प्रतिस्थापित ।

[2] 2009 के अधिनियम सं० 10 की धारा 35 द्वारा अंत:स्थापित ।

[3] 2009 के अधिनियम सं० 10 की धारा 36 द्वारा अंत:स्थापित ।

(क) साइबर घटना संबंधी सूचना का संग्रहण, विश्लेषण और प्रसार;

(ख) साइबर सुरक्षा घटनाओं का पूर्वानुमान और चेतावनियां;

(ग) साइबर सुरक्षा घटनाओं से निपटाने के लिए आपात अध्युपाय;

(घ) साइबर घटना मोचन क्रियाकलापों का समन्वय;

(ङ) साइबर घटनाओं की सूचना सुरक्षा पद्धतियों, प्रक्रियाओं, निवारण, मोचन और रिपोर्ट करने के संबंध में मार्गदर्शक सिद्धांत, सलाह, अति संवेदनशील टिप्पण और श्वेतपत्र जारी करना;

(च) साइबर सुरक्षा से संबंधित ऐसे अन्य कृत्य, जो विहित किए जाएं ।

(5) उपधारा (1) में निर्दिष्ट अभिकरण के कृत्यों और कर्तव्यों का पालन करने की रीति वह होगी, जो विहित की जाए ।

(6) उपधारा (4) के उपबंधों को कार्यान्वित करने के लिए, उपधारा (1) में निर्दिष्ट अभिकरण सेवा प्रदाताओं, मध्यवर्तियों, डाटा केंद्रों, निगमित निकायों और किसी अन्य व्यक्ति से सूचना मांग सकेगा और उसे निदेश दे सकेगा ।

(7) ऐसा कोई सेवा प्रदाता, मध्यवर्ती डाटा केंद्र, निगमित निकाय और अन्य व्यक्ति, जो उपधारा (6) के अधीन मांगी गई सूचना देने में या निदेश का अनुपालन करने में असफल रहता है, कारावास से, जिसकी अवधि एक वर्ष तक की हो सकेगी या जुर्माने से, जो एक लाख रुपए तक का हो सकेगा या दोनों से, दंडनीय होगा ।

(8) कोई न्यायालय, इस धारा के अधीन किसी अपराध का संज्ञान, उपधारा (1) में निर्दिष्ट अभिकरण द्वारा इस निमित्त प्राधिकृत किसी अधिकारी द्वारा दिए गए किसी परिवाद पर के सिवाय नहीं करेगा ।]

**71. दुर्व्यपदेशन के लिए शास्ति**—जो कोई, नियंत्रक या प्रमाणकर्ता प्राधिकारी के समक्ष, यथास्थिति, कोई अनुज्ञप्ति या [1][इलैक्ट्रानिक चिह्नक] प्रमाणपत्र प्राप्त करने के लिए कोई दुर्व्यपदेशन करता है या किसी तात्त्विक तथ्य को छिपाता है तो वह ऐसे कारावास से, जिसकी अवधि दो वर्ष तक की हो सकेगी, या ऐसे जुर्माने से, जो एक लाख रुपए तक का हो सकेगा, अथवा दोनों से, दण्डित किया जाएगा ।

**72. गोपनीयता और एकांतता भंग के लिए शास्ति**—इस अधिनियम या तत्समय प्रवृत्त किसी अन्य विधि में जैसा अन्यथा उपबंधित है उसके सिवाय, यदि किसी व्यक्ति ने, इस अधिनियम, इसके अधीन बनाए गए नियमों या विनियमों के अधीन प्रदत्त किन्हीं शक्तियों के अनुसरण में किसी इलैक्ट्रानिक अभिलेख, पुस्तक, रजिस्टर, पत्राचार, सूचना, दस्तावेज या अन्य सामग्री से सम्बद्ध व्यक्ति की सहमति के बिना पहुंच प्राप्त कर ली है, और वह किसी व्यक्ति को उस इलैक्ट्रानिक अभिलेख, पुस्तक, रजिस्टर, पत्राचार, सूचना, दस्तावेज या अन्य सामग्री को प्रकट करता है तो वह ऐसे कारावास से, जिसकी अवधि दो वर्ष तक हो सकेगी, या ऐसे जुर्माने से, जो एक लाख रुपए तक का हो सकेगा, अथवा दोनों से, दण्डित किया जाएगा ।

[2][**72क. विधिपूर्ण संविदा का भंग करते हुए सूचना के प्रकटन के लिए दंड**—इस अधिनियम या तत्समय प्रवृत किसी अन्य विधि में यथा उपबंधित के सिवाय, कोई व्यक्ति, जिसके अंतर्गत मध्यवर्ती भी है, जिसने, विधिपूर्ण संविदा के निबंधनों के अधीन सेवाएं उपलब्ध कराते समय, ऐसी किसी सामग्री तक, जिसमें किसी अन्य व्यक्ति के बारे में व्यक्तिगत सूचना अंतर्विष्ट है, पहुंच प्राप्त कर ली है, सदोष हानि या सदोष अभिलाभ कारित करने के आशय से या यह जानते हुए कि उसे सदोष हानि या सदोष अभिलाभ कारित होने की संभावना है, संबंधित व्यक्ति की सम्मति के बिना या किसी विधिपूर्ण संविदा का भंग करते हुए किसी अन्य व्यक्ति को ऐसी सामग्री प्रकट करता है, तो वह कारावास से, जिसकी अवधि तीन वर्ष तक की हो सकेगी, या जुर्माने से, जो पांच लाख रुपए तक का हो सकेगा, या दोनों से, दंडित किया जाएगा ।]

**73. [1][इलैक्ट्रानिक चिह्नक] प्रमाणपत्र की कतिपय विशिष्टियों को मिथ्या प्रकाशित करने के लिए शास्ति**—(1) कोई व्यक्ति, [1][इलैक्ट्रानिक चिह्नक] प्रमाणपत्र को तब तक प्रकाशित नहीं करेगा या किसी अन्य व्यक्ति को अन्यथा उपलब्ध नहीं कराएगा, यदि उसे यह जानकारी है कि—

(क) प्रमाणपत्र में सूचीबद्ध प्रमाणकर्ता प्राधिकारी ने उसे जारी नहीं किया है; या

(ख) प्रमाणपत्र में सूचीबद्ध हस्ताक्षरकर्ता ने उसे स्वीकार नहीं किया है; या

(ग) वह प्रमाणपत्र प्रतिसंहृत या निलम्बित कर दिया गया है,

जब तक कि ऐसा प्रकाशन, ऐसे निलम्बन या प्रतिसंहरण से पूर्व सृजित [1][इलैक्ट्रानिक चिह्नक] के सत्यापन के प्रयोजनार्थ न हो ।

(2) ऐसा कोई व्यक्ति, जो उपधारा (1) के उपबंधों का उल्लंघन करता है, ऐसे कारावास से जिसकी अवधि दो वर्ष तक हो सकेगी, या ऐसे जुर्माने से, जो एक लाख रुपए तक का हो सकेगा, अथवा दोनों से, दण्डित किया जाएगा ।

---

[1] 2009 के अधिनियम सं० 10 की धारा 2 द्वारा प्रतिस्थापित ।

[2] 2009 के अधिनियम सं० 10 की धारा 37 द्वारा अंत:स्थापित ।

**74. कपटपूर्ण प्रयोजन के लिए प्रकाशन**—जो कोई, किसी कपटपूर्ण या विधिविरुद्ध प्रयोजन के लिए कोई [1][इलैक्ट्रानिक चिह्नक] प्रमाणपत्र जानबूझकर सृजित करता है, प्रकाशित करता है या अन्यथा उपलब्ध कराता है, वह कारावास से, जिसकी अवधि दो वर्ष तक की हो सकेगी, या जुर्माने से, जो एक लाख रुपए तक का हो सकेगा, या दोनों से, दंडित किया जाएगा ।

**75. अधिनियम का भारत से बाहर किए गए अपराधों और उल्लंघनों को लागू होना**—(1) उपधारा (2) के उपबंधों के अधीन रहते हुए, इस अधिनियम के उपबंध, किसी व्यक्ति द्वारा भारत से बाहर किए गए किसी अपराध या उल्लंघन को भी, उसकी राष्ट्रिकता को विचार में लाए बिना, लागू होंगे ।

(2) उपधारा (1) के प्रयोजनों के लिए, यह अधिनियम किसी व्यक्ति द्वारा भारत से बाहर किए गए किसी अपराध या उल्लंघन को लागू होगा, यदि उस कार्य या आचरण में, जिससे यह अपराध या उल्लंघन होता है, भारत में अवस्थित कोई कंप्यूटर, कंप्यूटर, प्रणाली या कंप्यूटर नेटवर्क अंतर्वलित हो ।

**76. अधिहरण**—कोई ऐसा कंप्यूटर, कंप्यूटर प्रणाली, फ्लापी, काम्पैक्ट डिस्क, टेप चालन या उससे संबंधित कोई ऐसे अन्य उपसाधन, जिनकी बाबत इस अधिनियम, इसके अधीन बनाए गए नियमों, किए गए आदेशों या बनाए गए विनियमों के किसी उपबंध का उल्लंघन किया गया हो या किया जा रहा है, अधिहरणीय होंगे :

परन्तु जहां अधिहरण का अधिनिर्णय देने वाले न्यायालय के समाधानप्रद रूप में यह सिद्ध हो जाता है कि वह व्यक्ति, जिसके कब्जे, शक्ति या नियंत्रण में कोई ऐसा कंप्यूटर, कंप्यूटर प्रणाली, फ्लापी, काम्पैक्ट डिस्क, टेप चालन या उससे संबंधित कोई अन्य उपसाधन पाया जाता है, इस अधिनियम, इसके अधीन बनाए गए नियमों, किए गए आदेशों या बनाए गए विनियमों के उपबंधों के उल्लंघन के लिए उत्तरदायी नहीं है वहां न्यायालय, ऐसे कंप्यूटर, कंप्यूटर प्रणाली, फ्लापी, काम्पैक्ट डिस्क, टेप चालन या उससे संबंधित किसी अन्य उपसाधन के अधिहरण का आदेश करने के बजाय इस अधिनियम या इसके अधीन बनाए गए नियमों, किए गए आदेशों या बनाए गए विनियमों के उपबंधों का उल्लंघन करने वाले व्यक्ति के विरुद्ध इस अधिनियम द्वारा प्राधिकृत ऐसा अन्य आदेश कर सकेगा, जो वह ठीक समझे ।

[2][**77. प्रतिकर शास्ति या अधिहरण का अन्य दंड में हस्तक्षेप न करना**—इस अधिनियम के अधीन अधिनिर्णीत प्रतिकर, अधिरोपित शास्ति या किया गया अधिहरण, तत्समय प्रवृत्त किसी अन्य विधि के अधीन किसी प्रतिकर के अधिनिर्णय या किसी अन्य शास्ति या दंड के अधिरोपण को निवारित नहीं करेगा ।

**77क. अपराधों का शमन**—(1) सक्षम अधिकारिता वाला न्यायालय, उन अपराधों से भिन्न अपराधों का शमन कर सकेगा, जिनके लिए इस अधिनियम के अधीन आजीवन या तीन वर्ष से अधिक के कारावास के दंड का उपबंध किया गया है :

परंतु न्यायालय, ऐसे अपराध का वहां शमन नहीं करेगा, जहां अपराधी, उसकी पूर्व दोषसिद्धि के कारण या तो वर्धित दंड का या भिन्न प्रकार के किसी दंड के लिए दायी है :

परंतु यह और कि न्यायालय ऐसे किसी अपराध का शमन नहीं करेगा, जहां ऐसा अपराध देश की समाजिक-आर्थिक स्थिति पर प्रभाव डालता है या अठारह वर्ष की आयु से कम आयु के किसी बालक या किसी स्त्री के संबंध में किया गया है ।

(2) इस अधिनियम के अधीन किसी अपराध का अभियुक्त व्यक्ति उस न्यायालय में, जिसमें अपराध विचारण के लिए दंडित है, शमन के लिए आवेदन फाइल कर सकेगा और दंड प्रक्रिया संहिता, 1973 (1974 का 2) की धारा 265ख और धारा 265ग के उपबंध लागू होंगे ।

**77ख. तीन वर्ष के कारावास वाले अपराधों का जमानतीय होना**—दंड प्रक्रिया संहिता, 1973 (1974 का 2) में किसी बात के होते हुए भी, तीन वर्ष और उससे अधिक के कारावास से दंडनीय अपराध संज्ञेय होंगे और तीन वर्ष तक के कारावास से दंडनीय अपराध जमानतीय होंगे ।]

**78. अपराधों का अन्वेषण करने की शक्ति**—दंड प्रक्रिया संहिता, 1973 (1974 का 2) में अंतर्विष्ट किसी बात के होते भी, कोई ऐसा पुलिस अधिकारी, जो [3][निरीक्षक] की पंक्ति से नीचे का न हो, इस अधिनियम के अधीन किसी अपराध का अन्वेषण करेगा ।

[4]**[अध्याय 12**

## कतिपय मामलों में मध्यवर्तियों का दायी न होना

**79. कतिपय मामलों में मध्यवर्ती को दायित्व से छूट**—(1) तत्समय प्रवृत्त किसी विधि में अंतर्विष्ट किसी बात के होते हुए भी, किंतु उपधारा (2) और उपधारा (3) के उपबंधों के अधीन रहते हुए, मध्यवर्ती, उसको उपलब्ध कराई गई या परपोषित की गई किसी अन्य व्यक्ति की सूचना, डाटा या संसूचना संपर्क के लिए दायी नहीं होगा ।

(2) उपधारा (1) के उपबंध तभी लागू होंगे, जब—

---

[1] 2009 के अधिनियम सं० 10 की धारा 2 द्वारा प्रतिस्थापित ।

[2] 2009 के अधिनियम सं० 10 की धारा 38 द्वारा प्रतिस्थापित ।

[3] 2009 के अधिनियम सं० 10 की धारा 39 द्वारा प्रतिस्थापित ।

[4] 2009 के अधिनियम सं० 10 की धारा 40 द्वारा प्रतिस्थापित ।

# "साइबर सुरक्षित भारत"

**भारत में साइबर सुरक्षा प्रणाली को सुदृढ़ बनाने की आवश्यकता महसूस करते हुए तथा 'डिजिटल इंडिया' के विज़न के अनुरूप, इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) द्वारा राष्ट्रीय ई-गवर्नेंस डिविज़न (एनईजीडी) एवं उद्योग जगत के सहयोग से साइबर सुरक्षित भारत पहल की घोषणा की गई।**

**इसके माध्यम से सभी सरकारी विभागों में मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) एवं अग्रिम पंक्ति के आईटी कर्मचारियों के लिये सुरक्षा उपायों हेतु क्षमता निर्माण करने एवं साइबर अपराध के बारे में जागरूकता फैलाने का कार्य किया जाएगा।**

**इस मिशन का परिचालन जागरूकता, शिक्षा एवं सक्षमता के तीन सिद्धांतों पर किया जाएगा।**

**इसमें साइबर सुरक्षा के महत्त्व पर एक जागरूकता कार्यक्रम, सर्वश्रेष्ठ प्रचलनों पर कार्यक्रम की एक श्रृंखला तथा साइबर खतरों को प्रबंधित करने तथा इनमें कमी लाने के लिये साइबर सुरक्षा हेल्थ टूल किट्स के साथ अधिकारियों की सक्षमता जैसे पक्षों को शामिल किया गया है।**

**साइबर सुरक्षित भारत अपनी तरह की पहली सार्वजनिक-निजी साझीदारी है और यह साइबर सुरक्षा में आईटी उद्योग की विशेषज्ञता का लाभ उठाएगा।**

**देश के साइबर स्पेस की सुरक्षा सुनिश्चित करना डिजिटल इंडिया के विज़न का सबसे अहम् पक्ष है। वस्तुतः इसका उद्देश्य यह है कि विकास का लाभ समाज के प्रत्येक व्यक्ति तक पहुँचना चाहिये। डिजिटल इंडिया की वज़ह से अभिशासन प्रणाली में त्वरित रूपांतरण हुआ है। अत: सुशासन व्यवस्था को सुनिश्चित करने के लिये निश्चित रूप से निजी क्षेत्र की कपंनियों को आगे आना होगा, ताकि भविष्य के संदर्भ में इसकी राह को और अधिक दृढ बनाया जा सके।**

**वर्तमान में भारत में 118 करोड़ से अधिक आधार खाते मौजूद हैं जो लोगों को एक विशिष्ट पहचान उपलब्ध कराते हैं। जो इस बात को स्पष्ट करता है कि जैसे-जैसे हम आर्थिक संवृद्धि की तरफ बढ़ते जाते हैं, वैसे-वैसे हमें निश्चित रूप से यह सुनिश्चित करते जाना चाहिये कि हमारी डिजिटल व्यवस्था उसी के अनुरूप सुरक्षित रहे और हमारे डाटा की ठीक से हिफाज़त सुनिश्चित हो।**

**इस चिंता को ध्यान में रखते हुए भारत सरकार द्वारा साइबर सुरक्षित भारत पहल लॉन्च की गई है जिसका मुख्य उद्देश्य हमारे डाटा को भली-भाँति सुरक्षित रखना है।**

**हालाँकि, इसके लिये सरकार के साथ-साथ उद्योग जगत की सर्वश्रेष्ठ प्रतिभाओं को भी एकजुट होकर एक सुरक्षित साइबर स्पेस सुनिश्चित करने की दिशा में कार्य करना चाहिये।**

## साइबर अपराधों से निपटने की दिशा में भारत के प्रयास

- **भारत में 'सूचना प्रौद्योगिकी अधिनियम**, 2000' **पारित किया गया जिसके प्रावधानों के साथ-साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिये पर्याप्त हैं।**
- **सूचना प्रौद्योगिकी अधिनियम** 2000 **की धाराएँ** 43, 43**ए**, 66, 66**बी**, 66 **सी**, 66**डी**, 66**ई**, 66**एफ**, 67, 67**ए**, 67**बी**, 70, 72, 72**ए तथा** 74 **हैकिंग और साइबर अपराधों से संबंधित हैं।**
- **इसके अंतर्गत** 2 **वर्ष से लेकर उम्रकैद तथा दंड अथवा जुर्माने का भी प्रावधान है। सरकार द्वारा 'राष्ट्रीय साइबर सुरक्षा नीति**, 2013' **जारी की गई जिसके तहत सरकार ने अति-संवेदनशील सूचनाओं के संरक्षण के लिये 'राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र** (National Critical Information Infrastructure protection centre-NCIIPC) **का गठन किया।**
- **सरकार द्वारा 'कंप्यूटर इमरजेंसी रिस्पॉन्स टीम** (CERT-In)' **की स्थापना की गई जो कंप्यूटर सुरक्षा के लिये राष्ट्रीय स्तर की मॉडल एजेंसी है।**
- **विभिन्न स्तरों पर सूचना सुरक्षा के क्षेत्र में मानव संसाधन विकसित करने के उद्देश्य से सरकार ने 'सूचना सुरक्षा शिक्षा और जागरूकता'** (Information Security Education and Awareness: ISEA) **परियोजना प्रारंभ की है।**
- **भारत सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्तम कार्य प्रणाली अपनाने के लिये अमेरिका, ब्रिटेन और चीन जैसे देशों के साथ समन्वय कर रहा है।**
- **अंतर-एजेंसी समन्वय के लिये 'भारतीय साइबर अपराध समन्वय केंद्र'** (Indian Cyber Crime Co-ordination Centre-I4C) **की स्थापना की गई है।**

## बुडापेस्ट कन्वेंशन क्या है?

**Budapest Convention on cyber crime**

- **हाल ही में साइबर अपराध के संबंध में बुडापेस्ट कन्वेंशन** (Budapest Convention on cyber crime) **पर हस्ताक्षर करने के लिये गृह मंत्रालय द्वारा साइबर अपराध** (cyber crime), **क्रांतिकारीकरण** (radicalization) **और डेटा सुरक्षा को बढ़ावा देने के लिये अंतर्राष्ट्रीय सहयोग की आवश्यकता पर बल दिया जा रहा है।**
- **बुडापेस्ट कन्वेंशन साइबर क्राइम पर एक कन्वेंशन है, जिसे साइबर अपराध पर बुडापेस्ट कन्वेंशन या बुडापेस्ट कन्वेंशन के नाम से जाना जाता है।**
- **यह अपनी तरह की पहली ऐसी अंतर्राष्ट्रीय संधि है जिसके अंतर्गत राष्ट्रीय कानूनों को सुव्यवस्थित करके, जाँच-पड़ताल की तकनीकों में सुधार करके तथा इस संबंध में विश्व के अन्य**

**देशों के बीच सहयोग को बढ़ाने हेतु इंटरनेट और कंप्यूटर अपराधों पर रोक लगाने संबंधी मांग की गई है।**

- **इस कन्वेंशन में** 56 **सदस्य हैं**, **जिनमें अमेरिका और ब्रिटेन जैसे देश भी शामिल हैं।**

**<u>सीसीटीएनएस क्या है?</u>**

**Crime and Criminal Tracking Network and Systems (CCTNS)**

- **जून** 2009 **में शुरू किया गया सीसीटीएनएस एक ऐसा प्रोजेक्ट है जिसका उद्देश्य पुलिस स्टेशनों के स्तर पर पुलिस की दक्षता और प्रभावशीलता को बढ़ाने हेतु एक व्यापक और एकीकृत प्रणाली तैयार करना है।**
- **सीसीटीएनएस** (CCTNS-Crime and Criminal Tracking Network & Systems) **सभी स्तरों पर**, **विशेष रूप से पुलिस स्टेशन स्तर पर दक्षता और प्रभावी पुलिस कार्रवाई करने के लिये ई-शासन के सिद्धांतों को अपनाते हुए एक व्यापक और एकीकृत प्रणाली पर आधारित व्यवस्था है।**
- **सीसीटीएनएस सरकार की राष्ट्रीय ई-गवर्नेंस योजना** (National e-Governance Plan of Govt) **के अंतर्गत एक मिशन मोड प्रोजेक्ट** (Mission Mode Project -MMP) **है।**

**सौजन्य: राष्ट्रीय कृषि और ग्रामीण विकास बैंक (नाबार्ड)**

# म.प्र. राज्य सहकारी बैंक (अपेक्स बैंक)

**न्यू मार्केट, टी.टी. नगर, भोपाल 462003**

**0755 – 2674701 & 0755 – 2674702**

The softcopy of this document can be accessed at **www.apexbank.in**