NSDL
Technology, Trust & Reach

# द फाईनेंशियल कैलिडोस्कोप

जनवरी 2020

## संपादक की ओर से

भारत तेजी से नगदीरहित अर्थ-व्यवस्था बनने की ओर बढ़ रहा है और इसलिए डिजिटल व्यवहार भी बढ़ रहे हैं। बहुत तेज़ होने वाले इन व्यवहारों में वित्तीय रूप से निपुण होना बेहद जरूरी है। हमारे न्यूज़लेटर का यह संस्करण आपको अपनी मेहनत की कमाई को सुरक्षित रखने में मदद करेगा।

इसमें कोई संदेह नहीं है कि पिछले कुछ दशकों में भारतीय बैंकिंग और निवेश की परिस्थितियां काफी विकसित हुई हैं, खासकर छोटे और खुदरा उपभोक्ताओं के लिए। इस क्षेत्र में तकनीक के आगमन ने इंटरनेट आधारित बैंकिंग समाधानों की एक नई पीढ़ी को जन्म दिया है। इसके अतिरिक्त, इसने फिनटेक कंपनियों को भी उभरते देखा है जो मोबाइल और ऐप-आधारित बैंकिंग, निवेश और ई-वॉलेट सेवाएं प्रदान करती हैं, जो पहले मौजूद नहीं थीं।

हालांकि इन सबने वित्तीय सेवाओं को अधिक सुलभ बनाया है, पर साथ ही इसने जालसाजों को अनजान उपभोक्ताओं को धोका देने का मौका भी दिया है। ग्राहकों में कम जागरूकता और सिस्टम में कुछ खामियों के कारण वित्तीय अपराधों में वृद्धि हुई है। आज हम में से ज्यादातर लोग अपने दोस्तों या रिश्तेदारों में ऐसे व्यक्ति को अवश्य जानते हैं जो किसी न किसी तरह के वित्तीय घोटाले का शिकार हुआ हो।

वित्तीय धोखाधड़ी एक बड़ा क्षेत्र है। समझने में आसानी के लिए हमने इसके स्रोतों और माध्यमों का उल्लेख किया है। आपकी मेहनत की कमाई को धोखाधड़ी के पारंपरिक और आधुनिक तरीकों से बचने के उपायों के साथ ही हमने वास्तविक जीवन के कुछ ऐसे उदाहरण प्रस्तुत किये हैं जो बताते हैं कि ऐसे घोटाले किस तरह से होते हैं। जैसा कि एक प्रसिद्ध उद्धरण है, इलाज से बचाव अच्छा, हमें उम्मीद है कि आपको न्यूज़लेटर उपयोगी लगेगा।

हमें यह बताते हुए खुशी हो रही है कि इस अंक से आपका पसंदीदा न्यूज़लेटर हिंदी में भी उपलब्ध है। हिंदी संस्करण हमारी वेबसाइट **https://nsdl.co.in/publications/nest.php** पर उपलब्ध है।

हमेशा की तरह, यदि आपके पास इस न्यूज़लेटर पत्र के बारे में कोई टिप्पणी या प्रतिक्रिया है, तो कृपया हमें **info@nsdl.co.in** पर लिखें।

**सादर,**

**टीम एनएसडीएल**

# मेहनत से कमाए गए धन की सुरक्षा करें

## बैंकिंग से संबंधित संकट

अधिकांश निवेशकों के लिए, बैंक जमा अपनी बचत को रखने के सबसे सामान्य तरीकों में से एक है। सुविधा और सुरक्षा की भावना, फिक्स्ड डिपाजिट, रिकरिंग डिपाजिट आदि को आदर्श वित्तीय साधन बनाते हैं। हालांकि, अन्य सभी निवेशों की तरह बैंकिंग प्रणाली में भी कुछ जोखिम शामिल हैं।

बैंक की विफलता तब होती है जब वह अपने भुगतान दायित्वों को पूरा करने में असमर्थ होता है या भारतीय रिजर्व बैंक द्वारा बंद किया जाता है। यदि बैंक विफल हो जाता है, तो लोग बैंक के पास रखी अपनी बचत / जमा राशि भी खो देते हैं। उन्हें केवल ₹ 1 लाख तक की राशि प्राप्त हो सकती है, जो डिपॉजिट इंश्योरेंस एंड क्रेडिट गारंटी कॉर्पोरेशन से बैंकों द्वारा लिए गए डिपॉजिट इंश्योरेंस द्वारा कवर की जाती है। (निकट भविष्य में यह सीमा बढ़कर ₹ 5 लाख होने जा रही है)। भारत में, हालांकि उदारीकरण के बाद से कोई अनुसूचित वाणिज्यिक बैंक विफल नहीं हुआ है, पर सहकारी बैंकों में ऐसे मामले सामने आए हैं।

कुछ महीनों पहले एक सहकारी बैंक के कई ग्राहकों को भारतीय रिजर्व बैंक द्वारा लगाए गए प्रतिबंधो की वजह से अपने डिपाजिट निकालने में मुश्किलों का सामना करना पड़ा। दुर्भाग्यवश, ऐसी घटनाएं पहले भी कई बार हो चुकी हैं इसलिये जमाकर्ताओं को कई संभव जोखिमों का ध्यान रखना चाहिए ।

भारतीय रिजर्व बैंक के पास एक विशेष प्रावधान है जो कुछ समस्याओं का सामना करने वाले जमाकर्ताओं के लिए सीमा से अधिक राशि निकालने की अनुमति देता है। खाताधारक इस प्रावधान का उपयोग चिकित्सा खर्च, शादी से संबंधित खर्च या स्कूल की फीस के भुगतान के लिए कर सकते हैं। ये प्रावधान वरिष्ठ नागरिकों, विधवाओं और विकलांग लोगों के लिए भी लागू हैं। अतिरिक्त राशि निकालने की सीमा विभिन्न समूहों के लिए अलग होती है और समय के साथ बदल सकती है। ऐसी सभी स्थितियों में, विवरण, शर्तें और अन्य जानकारी भारतीय रिजर्व बैंक द्वारा सर्कुलर में प्रकाशित की जाती हैं।

### याद रखिये

- एक बैंक के साथ संकट के मामले में अपने जोखिम को कम करने के लिए अपनी बचत को कई बैंकों में जमा करें।
- नया खाता खोलने के लिए बैंक का चयन करते समय, संस्था के वित्तीय स्वास्थ्य की जाँच करें। सिर्फ बेहतर ब्याज दर पर न जाएँ।
- संकट के दौरान, यदि आप किसी आपात स्थिति में अतिरिक्त धनराशि निकालना चाहते हैं, तो नकद निकासी सीमा के साथ-साथ भारतीय रिजर्व बैंक के निर्देशों का भी ध्यान रखें। आप ऐसे मामलों में **https://www.rbi.org.in** पर जा सकते हैं।

# अवैध योजनाएँ

## पोंजी योजनाएँ

पोंजी स्कीम एक ऐसा घोटाला है, जो असाधारण उच्च रिटर्न का वादा करके निवेशकों को लुभाता है। पोंजी योजना एक धोखाधड़ी है जो मौजूदा निवेशकों को नए निवेशकों से एकत्र किए गए धन का एक बड़ा हिस्सा भुगतान कराती है। आगे जाकर रिटर्न काल्पनिक हो जाते है और पूरी स्कीम निवेशकों का सारा पैसा लेकर डूब जाती है। पोंजी योजना का नाम चार्ल्स पोंजी के नाम पर है, जिसने 1920 के दशक में संयुक्त राज्य अमरीका में डाक टिकटों में निवेश की योजना के नाम पर निवेशकों को धोखा दिया था।

## अपंजीकृत सामूहिक निवेश योजनाएं (सीआईएस)

बहुत से लोगों ने ऐसी संदेहजनक निवेश योजनाओं के बारे में सुना होगा जिसमें आपको एक संपत्ति या भूमि में निवेश करने कहा जाता है । जिसके लिए आपको हर महीने किश्त के रूप में एक छोटी राशि का भुगतान करने की आवश्यकता होती है। इनमें से कुछ योजनाएं आपको एक मामूली मासिक राशि का निवेश करके कुछ अनोखी जगहों पर एक बाग या अवकाश गृह के सह-मालिक बनने की आशा देती हैं। यह सब आकर्षक लगता है, जबकि ये सभी अपंजीकृत सीआईएस हैं। ऐसी किसी भी योजना में निवेश करने का निर्णय लेने से पहले यह जाँच लें कि यह योजना सेबी के पास पंजीकृत है या नहीं। सेबी पंजीकृत सामूहिक निवेश प्रबंधन कंपनियों की सूची **https://www.sebi.gov.in/sebiweb/other/Otherction.do?doRecognised=yes** पर उपलब्ध है।

### याद रखिये

- निवेश करने से पहले, प्रवेश और निकास नियमों, शुल्कों, समयरेखा सहित प्रस्ताव को अच्छी तरह से समझ लें।
- कभी भी टिप्स, अफवाहों, कही-सुनी बातों के आधार पर निवेश न करें।
- हमेशा अपना अनुसंधान करें और जिनके साथ आप अपनी मेहनत की कमाई का निवेश करने जा रहे हैं, उनकी जांच करे।
- यदि आप निवेश करने के लिए नए हैं या कहाँ या कैसे निवेश करें, इसके बारे में अनिश्चित हैं, तो एक पंजीकृत निवेश सलाहकार / विशेषज्ञ से परामर्श करें। बुरे निवेश में अपना सारा पैसा गंवाने के बजाये थोड़ा परामर्श शुल्क देना बेहतर है।
- हमेशा पंजीकृत संस्थाओं के साथ सौदा करें।
- दलालों या अन्य बिचौलियों से सौदा करने के दौरान, दिए गए सभी निर्देशों / आदेशों का एक लिखित रिकॉर्ड (ईमेल या संदेश) रखें।
- कोई भी निवेश करने से पहले हमेशा प्रामाणिक स्रोतों से जानकारी प्राप्त करें।

## विभिन्न प्रकार की धोखाधड़ी को जानिये

धोखा देने के लिए धोखेबाजों द्वारा आमतौर पर अपनाई जाने वाली विभिन्न प्रकार के चालों को जानना और समझना महत्वपूर्ण है। अगर हम उनके तौर-तरीकों को जानते हैं, तो खुद को सुरक्षित रख सकते हैं।

### पहचान की चोरी

पहचान चोरी तब होती है जब कोई व्यक्ति धोखाधड़ी के लिए आपकी व्यक्तिगत जानकारी प्राप्त करता है और उसका उपयोग करता है। व्यक्तिगत विवरण जैसे जन्म तिथि, पैन, बैंक खाता संख्या, क्रेडिट / डेबिट कार्ड नंबर का कई तरीकों से दुरुपयोग किया जा सकता है। क्रेडिट कार्ड जारी करने से लेकर स्वयं के लिए धन निकालने तक, गंभीर अपराधों के लिए आपके नाम से खाते खोलना आदि, यह सब पहचान चोरी से संभव हो सकता है।

### फिशिंग या टेलीकॉलिंग घोटाला

यह एक बहुत ही सामान्य प्रकार का धोखा है जिसमें वैध प्रतीत होने वाले स्रोतों (जैसे नियामकों, बैंकों, बीमा कंपनियों, वित्तीय संस्थानों, वकीलों आदि) से ईमेल करना या आपके परिचितों की ओर से कॉल करना शामिल है। इन अपराधियों का उद्देश्य आपकी निजी जानकारी को झूठे बहानों के से प्राप्त करना होता है। ईमेल या कॉल एक नियमित प्रक्रिया या आकर्षक लगने वाले प्रस्ताव या कुछ मामलों में मदद की दलील देने के लिए किए जाते हैं।

एक वरिष्ठ न्यायाधीश से जुड़े चर्चित मामले में, माननीय न्यायाधीश ने अपने एक अच्छे दोस्त से कथित तौर पर एक ईमेल प्राप्त किया जिसमें एक स्वास्थ्य सम्बन्धी आपात स्थिति के लिए पैसे की मांग की गई थी। उन्हें एक बैंक खाते का विवरण दिया गया था जिसमें उनके दोस्त चाहते थे कि धन तत्काल हस्तांतरित किया जाए। चूंकि दोनों अच्छी तरह से परिचित थे, न्यायाधीश ने राशि तुरंत स्थानांतरित कर दी। न्यायाधीश को एक और ईमेल मिलने के बाद यह मामला सामने आया। इस बार वास्तव में उनके मित्र ने कहा कि उनका ईमेल खाता हैक हो गया था।

### याद रखिये

- यदि कोई ईमेल या संदेश संदेहास्पद लगता है, तो उस पर कार्रवाई करने से पहले स्रोत को सत्यापित करें। कभी-कभी, प्रेषक को कॉल करना और संदेश की जांच करना बेहतर हो सकता है।
- अपने पासवर्ड या पिन के रूप में स्पष्ट या ज्ञात तत्वों का उपयोग न करें जैसे जन्म तिथि, मोबाइल नंबर, घर का नंबर या पालतू जानवर का नाम।
- अपना पासवर्ड और पिन नियमित रूप से बदलें, जैसे महीने में एक बार।
- हमेशा अपने सभी स्टेटमेंट्स को चेक करें जैसे कि आपके बैंक अकाउंट्स, डीमैट अकाउंट्स, ई-वॉलेट्स, क्रेडिट और डेबिट कार्ड्स आदि।
- किसी भी विसंगति या अज्ञात या अनधिकृत लेनदेन के मामले में, तुरंत अपने बैंक या कार्ड जारीकर्ता को सूचित करें।
- सभी प्रमुख लेनदेन के लिए मोबाइल एसएमएस अलर्ट की सुविधा लें।
- ऐसे यूआरएल की जाँच करें जो वैध लग सकते हैं, लेकिन अलग या अतिरिक्त वर्ण या शब्दों के साथ लिखे गए हैं - उदाहरण के लिए **iciicibank.com** या **statesbankofindia-online.net.in**
- किसी भी अज्ञात अटैचमेंट को डाउनलोड न करें या अज्ञात स्रोतों के एप्लिकेशन इंस्टॉल न करें।
- स्पैम कॉल से बचने के लिए डू नॉट डिस्टर्ब (डीएनडी) सेवा के लिए अपना मोबाइल नंबर पंजीकृत करें।

## नकली भुगतान लिंक और क्यूआर कोड

ई-वॉलेट जैसे कि पेटीएम, फोनपे और डिजिटल भुगतान विकल्प जैसे कि यूपीआई और गूगलपे ऑनलाइन भुगतान करने और भुगतान प्राप्त करने हेतु सामान्य तरीका बन गए हैं। कभी-कभी अपराधी संभावित खरीददार होने का दिखावा करते हैं और ई-वॉलेट या यूपीआई का उपयोग करके, धन हस्तांतरित करने के नाम पर विक्रेता को पे रिक्वेस्ट लिंक या पुष्टि संदेश अथवा नकली क्यूआर कोड भेजते हैं। विक्रेता अक्सर भुगतानकर्ता के नाम को देखते हैं और लेनदेन को अधिकृत कर देते हैं। बाद में उन्हें पता चलता है कि धन उनके खाते में जमा होने के बजाय निकाल लिया गया है।

## केवाईसी धोखाधड़ी

वित्तीय धोखाधड़ी पर नकेल कसने के लिए, भारतीय रिजर्व बैंक और सेबी जैसे नियामकों ने नो योर कस्टमर (केवाईसी) प्रक्रिया को अनिवार्य कर दिया है। इसमें बैंक या वित्तीय संस्थान के साथ कई व्यक्तिगत और वित्तीय विवरण साझा करना शामिल है। कर्मचारी होने का दिखावा करने वाले धोखेबाज़, ग्राहकों से या तो कॉल करके या एक नकली लिंक भेजकर विवरण माँगते हैं। फिर इन विवरणों का उपयोग अपने स्वयं के खातों में धनराशि स्थानांतरित करने या ऑनलाइन लेनदेन करने के लिए किया जाता है। इस तरह के एक मामले में, एक वरिष्ठ सरकारी अधिकारी के साथ 6 लाख रूपए की ठगी हुई। उन्होंने फर्जी लिंक पर खाता विवरण और ओटीपी साझा किया जिसे केवाईसी अपडेट करने के लिए भेजा गया था।

**"RBI की एक रिपोर्ट के अनुसार वित्तीय वर्ष 2018-19 में भारतीय बैंकिंग प्रणाली में 71,500 करोड की धोखाधड़ी हुई हैं"**

### याद रखिये

- नई वित्तीय सेवाओं या सुविधाओं का उपयोग करने से पहले मानक प्रक्रियाओं को समझें। प्रस्तुत सुविधाओं से परिचित होने के लिए अपना कुछ समय निकालें।
- अपने कंप्यूटर या मोबाइल पर ओके या सबमिट बटन दबाने से पहले अजनबियों द्वारा साझा किए गए लिंक या क्यूआर कोड की हमेशा जांच करें।
- केवाईसी प्रक्रियाओं सहित सभी लेनदेन का संचालन या तो आधिकारिक वेबसाइट या ऐप पर या किसी अधिकृत एजेंट के माध्यम से करें (उन्हें सत्यापित करने के बाद)।
- किसी भी प्रकार की गड़बड़ी का अहसास होते ही अपने ई-वॉलेट या डिजिटल पेमेंट ऑपरेटर को सभी संदिग्ध गतिविधियों की सूचना दें।
- भले ही आपने पैसे नहीं खोए हों, किसी भी संदिग्ध संचार की सूचना संबंधित प्राधिकारी को दें। यह धोखाधड़ी रोकने में उनकी मदद करता है और अन्य उपयोगकर्ताओं को अलर्ट करता है।
- याद रखें कि कोई भी सरकारी विभाग, नियामक जैसे सेबी या भारतीय रिजर्व बैंक, बीमा कंपनी या बैंक या क्रेडिट कार्ड जारीकर्ता आदि कभी भी आपसे आपका पैन या बैंक खाता संख्या या उसके बारे में पूछने के लिए कॉल नहीं करेंगे।

## स्किमिंग या क्लोनिंग

यह एक ऐसी तकनीक है जिसका उपयोग घोटालेबाज आपके कार्ड का विवरण प्राप्त करने के लिए करते हैं ताकि इसका दुरुपयोग करने के इरादे से कार्ड की एक प्रति बनाई जा सके। सबसे आम तरीकों में से एक यह है कि कार्ड रीडर के लिए एक छोटा-सा उपकरण संलग्न करते हैं या पॉकेट-आकार के डिवाइस के माध्यम से कार्ड को स्वाइप करते हैं जो आपके कार्ड से डेटा को पढ़ता है। यह रेस्तरां, बार और मॉल जैसी भीड़-भाड़ वाली जगहों पर आम है जहाँ अपराधी खुद को कर्मचारियों के रूप में छिपा सकते हैं।

## फोन पर क्रेडिट कार्ड लेनदेन

हम में से कई लोग डेबिट या क्रेडिट कार्ड का उपयोग करके अपने अधिकांश भुगतान करने के लिए अभ्यस्त हो गए हैं। यह नकदी नहीं रखने की सुविधा प्रदान करता तो है, पर असुरक्षित तरीके से कार्ड का उपयोग करने से आपको वित्तीय धोखाधड़ी का शिकार भी होना पड सकता है। हाल ही में मुंबई में एक व्यक्ति को एक स्थानीय दुकान से शराब की होम डिलीवरी का आदेश देते समय धोखा दिया गया था। उस व्यक्ति ने इंटरनेट का उपयोग कर के दुकान की खोज की और एक नंबर पर कॉल किया जिसे उसने ऑनलाइन पाया। आदेश प्राप्त करने वाले व्यक्ति ने पीड़ित को अपने क्रेडिट कार्ड का विवरण देने के लिए आश्वस्त किया, फिर उसका उपयोग ₹ 1.25 लाख के तीन भुगतान करने के लिए किया गया।

### याद रखिये

- कभी भी अपना कार्ड नंबर, सीवीवी नंबर या पिन किसी को न दें।
- न तो कभी किसी फोन कॉल, एसएमएस या ईमेल पर कार्ड का विवरण साझा करें।
- यदि वायरलेस कार्ड मशीन उपलब्ध नहीं है, तो पेमेंट काउंटर पर जाकर स्वयं भुगतान करें। कार्ड और पिन किसी को भी न दें। बात यह है कि आपका डेबिट या क्रेडिट कार्ड कभी भी आपकी दृष्टि से बाहर नहीं होना चाहिए।
- यदि आप एक पुराने कार्ड का उपयोग कर रहें हैं, तो स्मार्ट चिप वाले कार्ड में अपग्रेड करें जो आपके कार्ड के डेटा को अतिरिक्त सुरक्षा प्रदान करता है।
- यदि आप कार्ड खो देते हैं या अज्ञात लेनदेन पाते हैं, तो अपने बैंक को सूचित करें और कार्ड को तुरंत ब्लॉक करवायें। इसे सुनिश्चित करने के लिए, अपने बैंक / कार्ड जारीकर्ता के हॉट लाइन नंबरों को हमेशा संभाल कर रखें।
- सभी कार्ड लेन-देन की एक टैब रखें (या तो शुल्क प्राप्तियों या एसएमएस अलर्ट के माध्यम से) और इसे लेन-देन विवरण के साथ हर महीने मिलान करें।
- अपना कार्ड नंबर टेलीफोन पर जहां दूसरे सुन सकते हैं, साझा न करें।
- एटीएम का उपयोग करते समय, पिन को अंकित करने के पहले, कृपया कीपैड को अपने हाथ से ढकने का प्रयास करें। यह किसी को भी छिपे हुए कैमरे का उपयोग करके पिन को रिकॉर्ड करने से रोक देगा।
- उन एटीएम का उपयोग करना हमेशा बेहतर होता है, जो किसी बैंक शाखा के पास स्थित या संरक्षित होते हैं। ऐसी जगहों पर गुप्त कार्ड क्लोनिंग डिवाइस / छुपा हुआ कैमरा लगाकर मशीन से छेड़छाड़ करने की संभावना कम होती है।
- अपने क्रेडिट कार्ड पर अपनी आवश्यकताओं के अनुसार विभिन्न प्रकार के खर्चों के लिए राशि सीमा निर्धारित करें। यह अनुचित खर्चों को एक वांछित सीमा से परे रोक देगा।
- यदि आपको देश से बाहर जाने की आवश्यकता नहीं है, तो अपने डेबिट और क्रेडिट कार्डकार्ड पर अंतर्राष्ट्रीय लेनदेन को अक्षम करवा दें।
- बैंक को नए डेबिट या क्रेडिट कार्ड जारी करने के लिए अनुरोध करें अगर आपने कुछ उच्च जोखिम वाले देशों की यात्रा करते समय अपने डेबिट या क्रेडिट कार्ड का उपयोग किया है।

## आपके कंप्यूटर और लैपटॉप की सुरक्षा

पुराने ऑपरेटिंग सिस्टम या इंटरनेट ब्राउज़र के पुराने संस्करणों के कारण होने वाली सुरक्षा खामियाँ अक्सर अपराधियों द्वारा आपके डेस्कटॉप कंप्यूटर या लैपटॉप में पहुंच प्राप्त करने के लिए उपयोग की जाती हैं। मालवेयर और ट्रैकिंग सॉफ़्टवेयर से अवगत रहें जो आपके सिस्टम से संवेदनशील जानकारी को लीक या संचारित कर सकता है। ऐसे दुर्भावनापूर्ण सॉफ्टवेयर्स आमतौर पर संलग्नक के रूप में छिपे होते हैं और कुछ मामलों में क्लिक या डाउनलोड होने पर ऑटो इंस्टॉल करने के लिए प्रोग्राम किए जाते हैं।

## आपके मोबाइल / टैब डिवाइस की सुरक्षा

ऊपर बताए गए कंप्यूटर के समान समस्याओं के अलावा, मोबाइल डिवाइस एक अजीबोगरीब और बहुत बड़ी चुनौती पेश करते हैं - गोपनीयता और व्यक्तिगत डेटा तक पहुंच। हर बार जब आप एक नया ऐप इंस्टॉल करते हैं, तो यह फोन पर विभिन्न प्रकार की सेवाओं और डेटा तक पहुंचने की अनुमति के लिए अनुरोध करता है। आपके द्वारा दी जाने वाली अनुमतियों के आधार पर, ऐप आपके सभी डेटा और आपके मोबाइल से जुड़े सभी खातों तक पहुँच प्राप्त कर सकता है।

### याद रखिये

- मालवेयर से बचाने के लिए अपने डिवाइस (लैपटॉप, डेस्कटॉप और मोबाइल) पर विश्वसनीय एंटी-वायरस और एंटी-स्पाइवेयर स्थापित करें।
- याद रखें कि एक समय स्थापना करना पर्याप्त नहीं है। इन सॉफ़्टवेयर को नियमित रूप से अद्यतन (अपडेट) करें और रिलीज़ होते ही नया सुरक्षा पैच लागू करें।
- एप को विभिन्न चीज़ों की अनुमति सोच समझ कर दें
- वित्तीय लेनदेन के लिए कंप्यूटर का उपयोग करते समय, सुनिश्चित करें कि वेबसाइट में डेटा एन्क्रिप्शन है। एक एन्क्रिप्टेड वेबसाइट के यूआरएल में **https** और उसके बगल में एक लॉक आइकन होता है।
- अपने कंप्यूटर या मोबाइल डिवाइस को बेचने से पहले, उन में से सभी व्यक्तिगत जानकारी मिटा दें और इसे फ़ैक्टरी सेटिंग्स पर रीसेट करें।
- वित्तीय लेनदेन के लिए सार्वजनिक वाईफाई या किसी भी खुले नेटवर्क का उपयोग न करें।

याद रखें, वित्तीय धोखाधड़ी कई मायनों में संभव है। जालसाज हमेशा लोगों का फायदा उठाने के नए तरीके खोजते रहते हैं। वे अपने तरीके बदलते रहते हैं और इसलिए खुद को अपडेट और तैयार रखना महत्वपूर्ण है। अंततः हमें अपनी मेहनत की कमाई को सुरक्षित रखने के लिए स्वयं ज़िम्मेदार होना चाहिए।

## प्रतिभागियों के लिए प्रशिक्षण कार्यक्रम

### प्रतिभागियों के लिए सीपीई कार्यक्रम

एनआईएसएम द्वारा मान्यता प्राप्त सतत व्यावसायिक शिक्षा (सीपीई) प्रदाता के रूप में एनएसडीएल पात्र संबद्ध व्यक्तियों के लिए विभिन्न मॉड्यूल में सीपीई प्रशिक्षण कार्यक्रम प्रदान करता है। जनवरी 2020 में, एनएसडीएल ने अहमदाबाद, मुंबई और नई दिल्ली में ऐसे पांच प्रशिक्षण कार्यक्रम आयोजित किए।

### एनएसडीएल द्वारा की गई निवेशक शिक्षा पहल

निवेशकों को निवेश के विभिन्न पहलुओं से अवगत कराने के लिए एनएसडीएल पूरे देश में निवेशक जागरूकता कार्यक्रम आयोजित करता है। अब तक, एनएसडीएल ने 3900 कार्यक्रमों का आयोजन किया है, जिसमें 3.79 लाख से अधिक निवेशकों ने भाग लिया है। इन कार्यक्रमों के दौरान निवेशकों से प्राप्त प्रतिक्रिया बेहद उत्साहजनक है। इन कार्यक्रमों की अनुसूची **https://nsdl.co.in/Investor-wareness-Programmes.php** पर प्रकाशित की जाती है। हमें आपके संगठन / संस्थान / समाज के लिए कार्यक्रमों का आयोजन करने में खुशी होगी। ऐसे कार्यक्रमों के बारे में **infonsdl.co.in** पर हमें लिखकर निवेशक शिक्षा पहल को आगे बढ़ाने में मदद करें।

अधिक शिक्षा, अधिक बुद्धिमानी।

सतत व्यावसायिक शिक्षा (सीपीई) पर प्रतिभागियों के लिए आगामी प्रशिक्षण कार्यक्रम

| अनु-क्रमांक | प्रशिक्षण की तिथि | प्रशिक्षण का स्थान | प्रशिक्षण कार्यक्रम का प्रकार |
|---|---|---|---|
| 1 | 20 मार्च, 2020 | मुंबई | सतत व्यावसायिक शिक्षा – डिपॉजिटरी ऑपरेशन मॉड्यूल |
| 2 | 21 मार्च, 2020 | कोलकाता | सतत व्यावसायिक शिक्षा – डिपॉजिटरी ऑपरेशन मॉड्यूल |
| 3 | 28 मार्च, 2020 | नई दिल्ली | सतत व्यावसायिक शिक्षा – डिपॉजिटरी ऑपरेशन मॉड्यूल |

* अनुसूची परिवर्तन के अधीन है।

## आगामी निवेशक जागरूकता कार्यक्रम

| | | | | | |
|---|---|---|---|---|---|
| 1 | 02-Mar-20 | Hotel Lemon Tree, M.G.B., Shanti Kunj, Malviya Nagar, Alwar - 301001, Rajasthan | Alwar | Rajasthan | 06.00 p.m. - 08.00 p.m. |
| 2 | 02-Mar-20 | Shri Venkateshwara University, Rajabpur, N.H.-24, Venkateshwara Nagar, Amroha, Amroha - 244236, Uttar Pradesh | Amroha | Uttar Pradesh | 01.00 p.m. - 03.00 p.m. |
| 3 | 03-Mar-20 | Arya Mahila T.T. College, Rundhia Nagar, Bharatpur - 321001, Rajasthan | Bharatpur | Rajasthan | 03.00 p.m. - 05.30 p.m. |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 04-Mar-20 | The International Hotel, Veekshanam Road, Mahatma Gandhi Road, Opp. Chennai Silks, Kacheripady, Kochi - 682035, Kerala | Kochi | Kerala | 05.00 p.m. - 07.00 p.m. |
| 5 | 06-Mar-20 | Hotel Mourya Inn, 4-356, Kurnool Road, Ongole - 523002, Andhra Pradesh | Ongole | Andhra Pradesh | 05.00 p.m. - 08.00 p.m. |
| 6 | 06-Mar-20 | 54-15, 18/4, Kdgo Colony, Road Number 1, Guru Nanak Colony, Vijayawada - 520008, Andhra Pradesh | Vijayawada | Andhra Pradesh | 10.00 a.m. - 01.00 p.m. |
| 7 | 08-Mar-20 | Hotel K K Palace, Sagar Road, Near Bypass Road, Khurai - 470117, Madhya Pradesh | Khurai | Madhya Pradesh | 11.00 a.m. - 02.30 p.m. |
| 8 | 13-Mar-20 | Maa Ambe Hotel, Near Ajanta Steel, Samastipur - 848101, Bihar | Samastipur | Bihar | 12.00 p.m. - 03.00 p.m. |
| 9 | 14-Mar-20 | Clark Inn, P N M Mall, Patlipitra, Patna - 800013, Bihar | Patna | Bihar | 12.00 p.m. - 03.00 p.m. |
| 10 | 15-Mar-20 | Park Hotel, Dumraon - Buxar, Near Railway Station, Dumraon - 802119, Bihar | Dumraon | Bihar | 05.00 p.m. - 08.00 p.m. |
| 11 | 15-Mar-20 | Super 60 Classes, Kudra - Kaimur, Near Kudra Railway Station, Rohtas - 821101, Bihar | Rohtas | Bihar | 10.00 a.m. - 01.00 p.m. |
| 13 | 27-Mar-20 | K.L.E. Lingaraj College Of Business Administration, College Road, Belagavi - 590001, Karnataka | Belagavi | Karnataka | 10.00 a.m. - 03.00 p.m. |
| 14 | 28-Mar-20 | Hotel Sayaji, Near Bhimnath Bridge, Opp. Parsi Agyari, Sayajigunj, Vadodara - 390006, Gujarat | Vadodara | Gujarat | 06.00 p.m. - 09.00 p.m. |

* अनुसूची परिवर्तन के अधीन है। अद्यतन अनुसूची के लिए कृपया **https://nsdl.co.in/Investor-wareness-Programmes.php** पर जाएं।

# Knowledge Wins Contest

## What is the Bank Deposit Amount Covered Under Insurance?

To send your replies: visit/click www.nsdl.co.in/knowledge-win-contest.php
or
Scan this QR code

**25 Lucky Winners** get FREE GIFTS

## Previous Month's Winners

A. Arjun – Bangalore
Aakash Joshi – Bhavnagar
Abhinaba Pal – Burdwan
Abhishek K. Gairola – Dehradun
Abhishek Saha – Kolkata
Akhilesh Kumar – Bareilly
Anand Dave – Bangalore
Ashwani Goyal – Ambala
Ch. Suryanarayana – Anantapur
Chandresh Jain – Mumbai
Chetali Keni – Pune
Dharmik Shah – Mumbai
Dr. Moses Rajamani – Kancheepuram
Gaurav Gupta – Patna
Gururaj Rao – Mumbai
Hardeep Saini – Chohal
Hari Kumar B. – Bengaluru
Jagadeesh Rayala – Bangalore
Jithin Ram A. S. – Palakkad
Kamlesh Tarkhala – Porbandar
M. S. Vaidyanathan – Chennai
Manish Maru – Jamnagar
Mir Arif – Anantnag
Prasad S. Yelgodkar – Pune
Purnima D. Nath – Bangalore

Winners will soon receive their gifts on the address they have provided


***Head Office***

**Mumbai** : 4th Floor, 'A' Wing, Trade World, Kamala Mills Compound, Senapati Bapat Marg, Lower Parel, Mumbai - 400013 Tel.: (022) 24994200

***Branch Offices***

**Ahmedabad** **Bengaluru** **Chennai** **Hyderabad** **Kochi** **Kolkata** **New Delhi**

**For any grievance related to Demat account, you can email us at relations@nsdl.co.in**
**For any other information related to Demat account, you can email us at info@nsdl.co.in**


Terms & Conditions : 1) NSDL shall be solely responsible for the execution of this Contest. 2) This Contest is open to Indian Citizens only. 3) NSDL employees are not allowed to participate in this contest. 4) All personal details submitted must be accurate and complete and are subject to proof upon request by NSDL.
5) NSDL reserves the right to discontinue the contest at any given point of time without prior intimation. 6) All winners shall be selected by NSDL and the decision taken will be final.


Printed & Published by **Mr. Manoj Sathe** (Editor) on behalf of National Securities Depository Limited Investor Protection Fund Trust.