



इण्डियन ओवरसीज़ बैंक
Indian Overseas Bank

आपकी प्रगति का सच्चा साथी
Good people to grow with

ఫిషింగ్ అటాక్ నుండి నివారణకు చిట్కాలు

చేయవలసినవి

- ఏవైనా అటాచ్‌మెంట్‌లను తెరవడం లేదా మీరు స్వీకరించే ఫైల్‌లను డౌన్‌లోడ్ చేయడంలో జాగ్రత్తగా ఉండండి.
- మీరు ఏదైనా వ్యక్తిగత సమాచారాన్ని నమోదు చేయడానికి/ఇవ్వడానికి ముందు పంపినవారి ఇమెయిల్ ఐడి జాగ్రత్తగా చూడండి.
- యాంటీవైరస్, యాంటిస్పైవేర్ మరియు ఫైర్‌వాల్ సాఫ్ట్‌వేర్‌లను ఉపయోగించండి (వాటిని కూడా క్రమం తప్పకుండా నవీకరించండి).
- మీ వెబ్ బ్రౌజర్‌ను ఎల్లప్పుడూ అప్‌డేట్ చేయండి.
- మీరు ఏదైనా అనుమానాస్పద ఇమెయిల్‌ను/ సంక్షిప్త సందేశం స్వీకరిస్తే, అది చట్టబద్ధమైనదో కాదో నిర్ధారించడానికి బ్యాంక్‌కి వెంటనే కాల్ చేయండి

సూచనా सुरक्षा विभाग Information Security Department

केन्द्रीय कार्यालय 763 अन्ना सलाई चेन्नई - 600002, Central Office 763 Anna Salai, Chennai - 600002

చేయకూడనివి

- వ్యక్తిగత లేదా ఆర్థిక సమాచారం కోసం అడిగే ఇ-మెయిల్ లేదా పాప్-అప్ సందేశానికి ప్రత్యుత్తరం ఇవ్వవద్దు.
- ఇ-మెయిల్ ద్వారా వ్యక్తిగత లేదా ఆర్థిక సమాచారాన్ని అంటే క్రెడిట్ కార్డ్ లేదా ఇతర సున్నితమైన సమాచారాన్ని ఇమెయిల్ చేయవద్దు.
- మీరు ఆశించని లేదా అవసరం లేని ఇమెయిల్ లేదా నోఫీస్ మీడియా సందేశాలపై క్లిక్ చేయవద్దు.
- మీకు ఏదైనా అనుమానం ఉన్న ఈ-మెయిల్ చట్టబద్ధమైనది అని తెరవకండి. అది చట్టబద్ధమైనది మరియు మిమ్మల్ని సంప్రదించడానికి ప్రయత్నిస్తున్న వ్యక్తి నిజంగా అవసరమైతే, వారు మరొక పద్ధతిని ప్రయత్నిస్తారు.
- మీరు ఊహించని జోడింపులను తెరవకండి, ముఖ్యంగా జిప్ ఫైల్లు మరియు .exe ఫైల్లను ఎప్పుడూ అమలు చేయవద్దు.
- వ్యక్తిగత విషయాల కోసం మీ కంపెనీ ఇ-మెయిల్ చిరునామాను ఉపయోగించవద్దు.
- స్పామ్ ఇ-మెయిల్ను తెరవవద్దు.

- ఫిషింగ్ యొక్క ప్రధాన లక్ష్యం సోషల్ నెట్వర్కింగ్ కాబట్టి సోషల్ నెట్వర్కింగ్ సైట్లలో అనుమానాస్పద వీడియోలు లేదా చిత్రాలను తెరవవద్దు.
- బ్యాంక్ వివరాలను అడిగే ఫోన్ కాల్లకు ఎప్పుడూ స్పందించవద్దు. ఇది విషింగ్ (వాయిస్ ఫిషింగ్) కావచ్చు.
- మీరు "దొంగిలించబడిన" లేదా "పోగొట్టుకున్న" ఖాతా సమాచారాన్ని నిర్ధారించమని మిమ్మల్ని కోరుతూ ఏదైనా సందేశం(sms) అందుకుంటే ప్రతిస్పందించవద్దు