

మొబైల్ వాలెట్

అవగాహనా కార్యక్రమ భాగస్వాములు



ఆన్‌లైన్ మరియు మొబైల్ బ్యాంకింగ్

USSD చెల్లింపులు

చేయాల్సినవి:

- వెరిఫై చేసిన, విశ్వసనీయ వాలెట్ యాప్స్‌ను మాత్రమే ఎల్లప్పుడూ ఇన్‌స్టాల్ చేసుకోండి
- మీ ఫోన్ పిన్ ద్వారా సురక్షితంగా ఉందో లేదో నిర్ధారించుకోండి
- లావాదేవీలు జరపబోయే ముందు లబ్ధిదారుని మొబైల్ నెంబర్ సరిగా ఉందో లేదో నిర్ధారించుకోండి

చేయకూడనివి:

- అన్ని వాలెట్లకు ఒకే పాస్‌వర్డ్ వాడే పద్ధతిని అరికట్టండి
- చెల్లింపులు చేయడానికి ఓపెన్ వై-ఫై లేదా ధృవీకరించని డివైజ్‌లను వాడకండి
- అవిశ్వసనీయ QR కోడ్‌లను స్కాన్ చేయకండి

Follow us

dsci_connect
 dsci.connect

dsci-security-council-of-India

DIGITAL PAYMENT

Suraksha

A Joint Initiative of

DSCI | Google

PROMOTING DATA PROTECTION

"Digital money will empower the poor"

- Narendra Modi Prime Minister

డిజిటల్ సేమెంట్

#SaralBhiSecureBhi

డిజిటల్ చెల్లింపులు జరిపేటప్పుడు చేయాల్సిన మరియు చేయకూడని విషయాలను ఈ హ్యాండి బుక్‌లెట్ ద్వారా తెలుసుకోండి.

www.dsci.in/digital-payment-suraksha

చేయాల్సినవి:

- కేవలం విశ్వసనీయ మరియు ధృవీకరించిన బ్రౌజర్లు మరియు HTTPS రక్షిత వెబ్‌సైట్‌లను మాత్రమే చెల్లింపుల కోసం వినియోగించండి
- తరచుగా మార్చడంతో పాటు అనుమానం పచ్చిన వెంటనే కూడా పాస్‌వర్డ్‌లను మార్చండి
- చెల్లింపులు జరిపే అప్లికేషన్‌లను (బ్యాంక్స్ / పేమెంట్ బ్యాంక్స్ / వాలెట్స్) సదా లేటెస్ట్ వెర్షన్‌తో అప్‌డేట్ చేసి ఉంచుకోండి

చేయకూడనివి:

- మీ ఫోన్లో లాగిన్ వివరాలను ఎప్పుడూ భద్రపరచకండి, అలాగే అవిశ్వసనీయ కియోస్క్‌లలో మీ వివరాలను ఎంటర్ చేయకండి
- పబ్లిక్ డివైజ్‌ల ద్వారా మరియు సురక్షితం కాని, ఓపెన్ నెట్‌వర్క్‌ల ద్వారా లావాదేవీలు జరపకండి
- మీ మొబైల్ బ్యాంకింగ్ పిన్ నంబరును ఎవరితోనైనా పంచుకోవడాన్ని నిరోధించండి

చేయాల్సినవి:

- ఏ లావాదేవీ జరపబోయే ముందైనా మొబైల్ మనీ ఐడెంటిఫైయర్ మరియు మొబైల్ నెంబర్‌ను నిర్ధారించుకోండి
- నిర్ణీత వ్యవధిలో మీ M-PIN ను మార్చుతున్నారో లేదో నిర్ధారించుకోండి
- ఇన్‌కమింగ్ USSD విజ్ఞప్తులపై దృష్టి పెట్టండి

చేయకూడనివి:

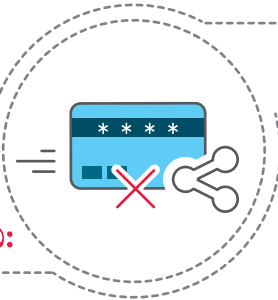
- మీ M-PIN ను ఇతరులతో పంచుకోవడం చేయరాదు
- మీ M-PIN ను ఎక్కడైనా రాయడాన్ని నిరోధించండి
- మీ OTP ని ఎవ్వరితోనూ పంచుకోరాదు

క్రెడిట్ మరియు డెబిట్ కార్డు



చేయాల్సినవి:

- మీ కార్డును వాడకం సమయంలో ఒక కంట కనిపెడుతూ ఉండండి, పని పూర్తయ్యాక తప్పనిసరిగా వెనక్కు తీసుకోండి
- లావాదేవీ SMS వివరాలు మరియు వాస్తవ లావాదేవీల మధ్య ఏమైనా తేడాలున్నాయేమో నిత్యం సరి చూసుకోండి
- రిసీట్లు మరియు స్టేట్మెంట్లను సురక్షితంగా పాఠవేశారో లేదో నిర్ధారించుకోండి.



చేయకూడనివి:

- మీ కార్డు సమాచారాన్ని భద్రపరిచే అవకాశం వ్యాపారులకు ఇవ్వకూడదు
- కార్డు యొక్క CVV మరియు పిన్లను ఇతరులతో పంచుకోవడాన్ని అరికట్టండి
- మీ క్రెడిట్ లేదా డెబిట్ కార్డును ఎవరి వద్దా వదిలివేయకండి

యూనిఫైడ్ పేమెంట్ ఇంటర్ఫేస్ మరియు BHIM



చేయాల్సినవి:

- చెల్లింపు చేయబోయే ముందు మర్చంట్తో పేమెంట్ కలెక్ట్ రిక్వెస్ట్ వివరాలను సరిచూసుకోండి
- యుపిఐ సంబంధిత యాప్స్ను తప్పనిసరిగా అప్డేట్ చేసుకోండి
- మీ డబ్బును పరిచిత లబ్ధిదారులకు మాత్రమే ట్రాన్స్ఫర్ చేశారో లేదో నిర్ధారించుకోండి



చేయకూడనివి:

- మీ యుపిఐ M-PINను ఇతరులతో పంచుకోవడంగానీ, ఎక్కడైనా రాయడం గానీ చేయకూడదు
- యుపిఐ / భీమ్ లావాదేవీలకు జైల్బ్రోకెన్ డివైజ్లను వాడడాన్ని అరికట్టండి
- లబ్ధిదారుడిని వెరిఫై చేయకుండా డబ్బును బదిలీ చేయడాన్ని నిరోధించండి

ఆధార్ ఆధారిత చెల్లింపు పద్ధతి



చేయాల్సినవి:

- డబ్బును బదిలీ చేసే ముందు ఆధార్ సంఖ్యను ఎల్లప్పుడూ వెరిఫై చేసుకోండి
- POS మరియు బయోమెట్రిక్ కాప్చర్ డివైజ్లతో లావాదేవీలు జరిపేటప్పుడు తప్పనిసరిగా ఆధార్ ఐడిని వాడండి
- (POS మరియు బయోమెట్రిక్ కాప్చర్ మెషిన్) డివైజ్లు టాంపర్ చేయబడలేదని, అలాగే కేవలం ధ్రువీకరించిన డివైజ్లను మాత్రమే వాడుతున్నారని నిర్ధారించుకోండి



చేయకూడనివి:

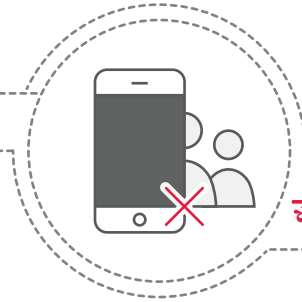
- మీ బయోమెట్రిక్స్ మరియు కార్డు వివరాలను వ్యాపారులు భద్రపరచకుండా నిరోధించండి
- మీ AEPS కార్డును పట్టించుకోకపోవడం లేదా మీ దృష్టిని దాటిపోకుండా ఉండడాన్ని నిరోధించండి
- సరైన కారణం లేకుండా మీ ఆధార్ మరియు వ్యక్తిగత వివరాలను ఎవరితోనూ పంచుకోకండి

ముఖ్యమైన ప్రాధమికాంశాలు



చేయాల్సినవి:

- మీ డివైజ్ను సదా అప్డేట్గా, బలమైన పాస్వర్డ్తో లాక్ చేసి సురక్షితంగా ఉంచుకోండి
- లావాదేవీ వివరాలు మరియు అలర్ట్లపై ఒక కన్నీసి ఉంచండి. ఏదైనా అనుమానాస్పద లేదా ఫ్రాడ్ జరిగిందని భావిస్తే సంబంధిత సర్వీస్ ప్రొవైడర్ మరియు పోలీస్ అధికారులకు రిపోర్ట్ చేయండి
- మీ డివైజ్ పోయిన లేదా దొంగిలించబడిన వెంటనే మీ సిమ్ను బ్లాక్ చేయండి. సంబంధిత బ్యాంక్/వాలెట్ సంస్థ మరియు పోలీస్ అధికారులకు సమాచారమివ్వండి
- మీ ఆర్థికపరమైన వివరాలు తదితర సున్నిత సమాచారాన్ని కోరుతూ వచ్చే అపరిచిత కాల్స్, మెసేజ్లు లేదా ఈమెయిల్స్ నుండి జాగ్రత్తగా ఉండండి
- ఫైర్ వాల్స్, వైరస్ మాలివేర్, చొరబాటును కనిపెట్టే వ్యవస్థ, మొబైల్ సెక్యూరిటీ సొల్యూషన్స్ వంటి ప్రమాదాలను పసిగట్టే మరియు తొలగించే అప్లికేషన్లను తప్పనిసరిగా ఇన్స్టాల్ చేసుకుని యాక్టివేట్ చేసి ఉంచుకోండి
- మంచి రివ్యూలు మాత్రమే ఉన్న ప్రామాణిక యాప్ స్టోర్ల నుండే మీ డివైజ్లలో అప్లికేషన్లు డౌన్లోడ్ చేసుకోండి
- బ్యాంకు వెబ్సైట్ల నుండి లింక్లను రూడి చేసుకోవడం ద్వారా అప్లికేషన్ల ప్రమాణికతను ధృవపరుచుకోండి



చేయకూడనివి:

- అడ్మినిస్ట్రేటివ్ (ప్రివిలేజెస్ ఉన్న) ఇంటర్నెట్ను ఎట్టి పరిస్థితుల్లో వాడరాదు
- SMS లేదా ఈమెయిల్లో ఇచ్చిన అనుమానాస్పద లింక్లను నొక్కడాన్ని నిరోధించండి
- నమ్మదగని, వెరిఫై చేయబడని సోర్స్ నుండి ఎట్టి పరిస్థితుల్లో యాప్లను ఇన్స్టాల్ చేయరాదు
- మొబైల్ బ్యాంకింగ్ కోసం జైల్ బ్రోకెన్ లేదా రూటెడ్ డివైజ్లను వాడడాన్ని అరికట్టండి
- ఆన్లైన్ డిజిటల్ చెల్లింపులకు సురక్షితం కాని వైఫై పాయింట్లకు కనెక్ట్ అవడాన్ని అరికట్టండి
- అపరిచిత సోర్స్ల నుండి అందే ఈమెయిల్స్ లేదా అటాచ్మెంట్లను తెరవడం లేదా డౌన్లోడ్ చేయకండి
- ఎట్టి పరిస్థితుల్లో మీ డివైజ్ను అపరిచితులకు అందించరాదు
- మీ డెబిట్ కార్డు / క్రెడిట్ కార్డు / ATM PIN / CVV / ఎక్స్ పైరి డేట్ లేదా పాస్వర్డ్స్ వంటి సమాచారాన్ని కోరుతూ వచ్చే అపరిచిత ఈమెయిల్స్, కాల్స్, మెసేజ్లు నుండి జాగ్రత్తగా ఉండండి