UPI చెల్లింపుల్లో మోసాలు - తీసుకోవల్సిన జాగ్రత్తలు

యూపీఐ లావాదేవీల మోసాలు జరగడానికి పోలీసులు ప్రధానంగా కొన్ని కారణాలు చెబుతున్నారు. అవేంటంటే.. తొలుత స్కామర్లు బాధితులకు మాయమాటలు చెప్పి రిమోట్ అసిస్టెన్స్ సాఫ్ట్‌వేర్లను డౌన్‌లోడ్ చేయిస్తున్నారు. దాంతో ఫోన్‌లోని సమాచారం మొత్తం వారి ఆధీనంలోకి వెళ్లిపోతుంది. వెంటనే హ్యాకర్లు తమ పని ప్రారంభించి ఈ-వ్యాలెట్లను నియంత్రణలోకి తెచ్చుకుంటారు. ఇలాంటి కేసుల్లో స్కామర్లు తమను తాము కస్టమర్ కేర్ ప్రతినిధులుగా బాధితులతో పరిచయం చేసుకుంటున్నారు. వెంటనే ఈకేవైసీ పూర్తి చేయాలని, లేని పక్షంలో వ్యాలెట్లు పని చేయవని తొందరపెడుతున్నారు. ఇంకొన్ని కేసుల్లో ఆధార్-పాన్ అనుసంధానం అంటూ బురిడీ కొట్టిస్తున్నారు. సైబర్ మోసగాళ్లకు వివరాలన్నీ చెప్పిన తరువాత ఓ థర్డ్ పార్టీ యాప్ డౌన్‌లోడ్ చేసుకోమని లింక్ పంపిస్తున్నారు. ఒక్కసారి ఆ యాప్ ఇన్‌స్టాల్ చేసుకోగానే వ్యాలెట్‌లోని మొత్తాన్ని దోచేస్తున్నారు.

ఈ నేపథ్యంలో ఎక్కువగా జరుగుతున్న యూపీఐ మోసాల తీరును పరిశీలించండి..

I. నకిలీ యూపీఐ రిక్వెస్ట్

ఈ విధానంలో నేరగాళ్లు ముందుగా కొంత మొత్తాన్ని బాధితుల యూపీఐ అకౌంట్‌లోకి పంపిస్తారు. ఆ తరువాత ఫోన్ చేసి పొరపాటున ఆ నగదు పంపించామని చెబుతారు. ఆ డబ్బుతో అత్యవసరంగా పని ఉందని, తిరిగి పంపించమని ప్రాధేయపడతారు. బాధితులు అందుకు ఓకే చెబితే రీఫండ్ పేరుతో సైబర్ నేరగాళ్లు మరో లింక్ పంపిస్తారు. దాన్ని క్లిక్ చేస్తే స్కామర్లు బాధితుల ఫోన్‌ను తమ ఆధీనంలోకి తెచ్చుకుని వ్యాలెట్, బ్యాంకు ఖాతాలోని నగదు దోచేస్తారు.

2. ఫేక్ క్యూఆర్ కోడ్

సైబర్ నేరగాళ్లు ఉపయోగిస్తున్న మరో టెక్నిక్ క్యూఆర్ కోడ్. ఈ విధానంలో క్యూఆర్ కోడ్ ద్వారా డబ్బులు వచ్చినట్లు బాధితులకు రిక్వెస్ట్ సందేశం పంపిస్తారు. ఆ క్యూఆర్ కోడ్‌ను స్కాన్ చేసి యూపీఐ పిన్ ఎంటర్ చేయగానే బాధితుల అకౌంట్‌లో నుంచే డబ్బులు డ్రా అయిపోతాయి.

ఎలాంటి జాగ్రత్తలు తీసుకోవాలి

యూపీఐ లావాదేవీలు నిజానికి చాలా భద్రమైనవి. ఓటీపీ, యూపీఐ పిన్ వివరాలు చెప్పనంత వరకు స్కామర్లు ఏమీ చేయలేరు. యూపీఐ మోసాల బారిన పడకుండా ఉండాలంటే..

- యూపీఐ పిన్‌ను ప్రతి నెల మార్చుకోవాలి.
- ఎవరైనా పొరపాటున నగదు పంపించి.. వెంటనే ఆ డబ్బు తిరిగి పంపించమని మరో లింక్ పంపిస్తే దాన్ని క్లిక్ చేయొద్దు. అవసరమైతే ఆ వ్యక్తి ఫోన్ నంబర్ తీసుకొని లావాదేవీలు పూర్తి చేయాలి.
- ఏటీఏం పిన్ లాగే యూపీఐ పిన్ చాలా ముఖ్యమైనది. దాన్ని ఎట్టి పరిస్థితుల్లోనూ ఇతరులతో పంచుకోవద్దు.
- కస్టమర్ కేర్ ప్రతినిధులు, మీకు తెలిసిన వారి స్నేహితులు, బంధువులు అని చెప్పి డబ్బులు అడుగుతూ సందేశం పంపించగానే లేదా ఫోన్ చేయగానే నమ్మకూడదు. పూర్తిగా నిర్ధారించుకున్న తరువాతే నిర్ణయం తీసుకోవాలి.
- ఆన్‌లైన్‌లో జరుగుతున్న కొత్త తరహా మోసాలపై అవగాహన పెంచుకోవాలి. మీ ఇంట్లో వారిని సైతం అప్రమత్తం చేయాలి.