వెలుగు లైఫ్
బుధవారం
07.08.2019
www.v6velugu.com
03.

అవేర్‌నెస్

ఓటీపీ చెప్పిన్రో బుక్కయిపోతరు

రాము ఏదో పనిలో చాలా బిజీగా ఉన్నాడు. అప్పుడే ఒక కాల్ వచ్చింది. అవతలి వ్యక్తి ఫలానా కస్టమర్ సర్వీస్ సెంటర్ నుంచి మాట్లాడుతున్నానని చెప్పాడు. మాటలు కలిపాడు. తర్వాత ‘సార్ మీ ఫోన్‌కు ఒక ‘ఓటీపీ’ వస్తుంది. చూసి చెప్పండి’ అన్నాడు. మాటల్లో పడి రాము ఆ ఓటీపీ చెప్పేశాడు. ఆ తర్వాత మరో మెసేజ్ వచ్చింది. ‘మీ వర్చువల్ వ్యాలెట్ (ఈ–వ్యాలెట్) బ్యాలెన్స్ జీరో’. అప్పుడు కానీ అర్థం కాలేదు రాముకు.. తాను మోసపోయానని.

ఇలాంటి మోసాలు రోజూ ఎక్కడో ఒక చోట జరుగుతూనే ఉన్నాయి. ఇప్పటి వరకు ఏటీఎం, క్రెడిట్‌కార్డ్, ఆన్‌లైన్ ట్రాన్సాక్షన్స్ విషయంలో ఇలాంటి మోసాలు జరిగేవి. కానీ.. ఇప్పుడు వర్చువల్ వ్యాలెట్‌లను కూడా వదలడంలేదు సైబర్ నేరగాళ్లు. అందుకే ఓటీపీ విషయంలో కాస్త జాగ్రత్తగా ఉంటే మంచిది.

స్మార్ట్‌ఫోన్ అందుబాటులోకి వచ్చిన తర్వాత టెక్నాలజీలో అనేక మార్పులు వచ్చాయి. అందరికీ ఎంతో కొంత టెక్ నాలెడ్జ్ ఉంటుంది. అయినా సైబర్ నేరగాళ్లు మోసాలు చేస్తూనే ఉన్నారు. ఎంతోమంది మోసపోతూనే ఉన్నారు. దీనికి ముఖ్య కారణం.. సైబర్ నేరగాళ్లు కూడా ఎప్పటికప్పుడు అప్‌డేటెడ్ టెక్నాలజీని ఉపయోగించడం. గతంలో ఫోన్ చేసి ఏదో రకంగా నమ్మించి, ఏటీఎం కార్డు వెనక ఉండే సీవీవీ, పిన్ అడిగి తెలుసుకునేవాళ్లు. తర్వాత చూస్తే అకౌంట్ ఖాళీ. స్మార్ట్‌ఫోన్‌లు అందుబాటులోకి వచ్చిన తర్వాత మొబైల్‌కు లింకులు పంపి, ఫోన్ చేసి ఆ లింకులపై క్లిక్ చేయమని ఫ్రాడ్ చేసేవాళ్లు ఫోన్ చేసి మాయమాటలు చెప్పి ఓటీపీ తెలుసుకుని డబ్బు కాజేయడం మొదలుపెట్టారు. ఇప్పుడు వాటితో పాటు వర్చువల్ వ్యాలెట్‌లను కూడా ఖాళీ చేసేస్తున్నారు.
గతంలో కార్డ్, క్యాష్ పేమెంట్లు ఉండేవి. కానీ.. ఇప్పుడు వర్చువల్ పేమెంట్స్ అందుబాటులోకి వచ్చాయి. అంటే మన బ్యాంక్ అకౌంట్ నుంచి ఈ-వ్యాలెట్‌లోకి డబ్బు ట్రాన్స్‌ఫర్ చేసుకుని షాపింగ్ చేసినప్పుడు ఈజీగా పే చెయ్యొచ్చు.

బీ అలెర్ట్

ఈ మోసాలు ఎలా ఉంటాయో.. ఈ ఎగ్జాంపుల్ చదివితే అర్థమవుతుంది. గురుగ్రామ్‌లోని ఒక ఫేమస్ బేకరీ నుంచి ఒకావిడకు కాల్ వచ్చింది. ఫోన్ చేసిన అతను ‘మీ ఆర్డర్ రెడీ.. కావాల్సిన టైంకు డెలివరీ చేస్తాం. కానీ.. అంతకంటే ముందు మీరు సగం బిల్లు పే చేయాల్సి ఉంటుంది. మిగతాది ఆర్డర్ డెలివరీ అయిన తర్వాత పే చేయండి’. అని చెప్పాడు. ఆమె బదులుగా వర్చువల్ వ్యాలెట్ నుంచి పే చేస్తానని చెప్పింది. అందుకోసం ఓటీపీ చెప్పాల్సి ఉంటుందని, కాల్‌లో ఉండగానే ఆమె ఫోన్‌కు ఒక ఓటీపీ పంపించాడు. దాంతో ఆమె ఏం ఆలోచించకుండా ఓటీపీ చెప్పేసింది. వెంటనే ఆమె పేటీఎం వ్యాలెట్ మొత్తం ఖాళీ అయ్యింది. ఆమె విషయం తెలుసుకునే లోపే జరగాల్సిన నష్టం మొత్తం జరిగిపోయింది. తిరిగి అదే నంబర్‌కు కాల్ చేస్తే స్విచాఫ్.. ఇలాంటివి ప్రతి రోజు ఎక్కడో ఒక చోట జరుగుతూనే ఉంటాయి. బెంగళూరులో జరిగిన మరో కేసు చూద్దాం.. ఒక క్రెడిట్ కార్డు కస్టమర్‌కు ఫోన్ చేసి ‘నేను బ్యాంక్ నుంచి కాల్ చేస్తున్నా.. మీ క్రెడిట్ కార్డ్ వివరాలు అప్‌డేట్ చేయడానికి మీ మొబైల్‌కు ఒక ఓటీపీ పంపుతున్నాం. అది మాకు చెప్పండి’ అని అడిగాడు. ఆ కస్టమర్ నిజమే అని నమ్మి ఓటీపీ చెప్పాడు. తర్వాత చూస్తే ఖాతా నుంచి చాలా డబ్బు మాయమైంది.
ఇలా చాలామంది తమ ఓటీపీలను షేర్ చేసుకోవడం వల్ల ఎంతో డబ్బు పోగొట్టుకుంటున్నారు. ముంబైలో ఉంటున్న ఒకావిడ అయితే 28సార్లు ఓటీపీ చెప్పి ఏకంగా ఏడు లక్షల రూపాయలు పోగొట్టుకుంది.

ఓటీపీ అంటే..

ఆన్‌లైన్ ట్రాన్సాక్షన్స్ చేసేటప్పుడు పేమెంట్‌ను యాక్సెప్ట్ చేసేందుకు రిజిస్టర్డ్ మొబైల్ నంబర్‌కు బ్యాంకు లేదా పేమెంట్ గేట్‌వే ఒక ఓటీపీ (వన్ టైం పాస్‌వర్డ్) నంబర్‌ను పంపిస్తుంది. ఆ ఓటీపీని వాళ్లు సూచించిన విధంగా ఎంటర్ చేస్తే పేమెంట్‌ను కన్ఫర్మ్ చేసినట్టు. అప్పుడే ఆ ట్రాన్సాక్షన్ పూర్తవుతుంది. ఈ ఓటీపీలకు కొంత టైం పీరియడ్ ఉంటుంది. ఆ టైం దాటితో అది ఎక్స్‌పైర్ అయిపోతుంది. అయితే ఓటీపీగా ఒక్కోసారి నంబర్‌తో పాటు లెటర్స్ కూడా రావొచ్చు.

ఓటీపీ ఎలా దొంగిలిస్తారు

సైబర్ నేరగాళ్లు ఓటీపీలను రెండు రకాలుగా తెలుసుకునే అవకాశం ఉంది. సాధారణంగా అయితే ఫోన్ చేసి నమ్మించి ఓటీపీ తెలుసుకుంటారు. కానీ.. కొన్ని సార్లు మాత్రం ఫోన్‌ను హ్యాక్ చేసి తెలుసుకుంటారు.

అదెలాగంటే.. మెయిల్, ఎస్ఎంఎస్ లేదా వాట్సాప్ ద్వారా ఒక లింక్‌ను పంపుతారు. దానిపై క్లిక్ చేయగానే అది బ్రౌజర్‌లో రీ డైరెక్ట్ అవుతుంది. అలా జరిగిన మరు క్షణం నుంచి ఫోన్ హ్యాక్ అయినట్టే.
అంటే ఫోన్‌లోని డాటా మొత్తం టెక్స్ట్ మెసేజ్‌లతో సహా హ్యాకర్లకు తెలుస్తుంది. అప్పుడు ఓటీపీ పంపి.. ఖాతాలు, వర్చువల్ వాలెట్స్ ఖాళీ చేస్తారు.

యాప్స్‌తో జాగ్రత్త

ఇప్పుడంతా స్మార్ట్‌ఫోన్ హవా నడుస్తోంది. ఏ ఇన్ఫర్మేషన్ కావాలన్నా దానికి సంబంధించిన యాప్‌ను డౌన్‌లోడ్ చేసుకుంటున్నారు. అయితే ఇలా థర్డ్ పార్టీ యాప్స్ ఇన్‌స్టాల్ చేసుకున్నప్పుడు అసలు ఏం చూడకుండానే అది పర్మిషన్లు అడగ్గానే ‘ఎలో’ బటన్‌పై క్లిక్ చేస్తుంటాం. అలా చేయడం వల్ల ఫోన్ యాక్సెస్‌ను మనమే స్వయంగా హ్యాకర్లకు ఇస్తున్నాం. అందుకే ఏ యాప్ ఇన్‌స్టాల్ చేసుకున్నా అది అడిగే పర్మిషన్లు, యాక్సెసెస్ అన్నింటినీ జాగ్రత్తగా చదివిన తర్వాతే ఇవ్వాలి. ఫిజికల్ లొకేషన్ లాంటివి ఆ యాప్ యూజ్ చేయడానికి తప్పనిసరిగా అవసరం అనుకుంటేనే ఇవ్వాలి.

కొత్త యూజర్లు, సీనియర్ సిటిజన్లే లక్ష్యం

ఆన్‌లైన్ పేమెంట్స్, ఇంటర్‌నెట్ వాడకంపై పెద్దగా అవగాహన లేనివాళ్లనే సైబర్‌నేరగాళ్లు టార్గెట్ చేస్తుంటారు. అంటే మొదటిసారి ఆన్‌లైన్ బ్యాంకింగ్‌ను వాడుతున్నవాళ్లను, టెక్నాలజీ పెద్దగా తెలియని వయసుపైబడిన వాళ్లను టార్గెట్ చేసుకుని ఓటీపీలు పంపి మోసాలు చేస్తుంటారు. అందుకే ఆన్‌లైన్, వర్చువల్ పేమెంట్స్, బ్యాంక్ ట్రాన్సాక్షన్స్‌పై అందరూ అవగాహన పెంచుకోవాలి. లేదంటే జేబు గుల్ల అవుతుంది.

ఏం చేయకూడదు, ఏం చేయాలి

- ఓటీపీ ఎవరితోనూ షేర్ చేసుకోవద్దు. బ్యాంకర్లు ఎప్పుడూ ఓటీపీలు అడగరు. అందుకే బ్యాంక్ ఖాతా వివరాల కోసం వచ్చే కాల్స్, ఈ-మెయిల్స్‌కు రిప్లై ఇవ్వొద్దు.
- సెక్యూర్ వెబ్ సైట్‌లలోనే షాపింగ్ చేయడం మంచిది. URLలో అంటే https:// అని ఉంటే అది సెక్యూర్ సైట్ అని నమ్మొచ్చు.
- వర్చువల్ వ్యాలెట్‌లను ఉపయోగించిన తర్వాత యాప్‌లో లాగవుట్ అవడం బెటర్.
- ఇతరుల డివైజ్‌లలో వర్చువల్ వ్యాలెట్ అకౌంట్లను లాగిన్ చేయొద్దు. ఒకవేళ చేసినా పని చేసుకున్న వెంటనే లాగవుట్ చేయాలి.
- ట్రాన్సాక్షన్ జరిగేటప్పుడు మాత్రమే ఓటీపీ వస్తుందని గుర్తుంచుకోవాలి.