పీడీఎఫ్ అమాంతం తెరవొద్దు

ఆఫీస్ డాక్యుమెంట్ కావచ్చు.. ఆఫర్ లెటర్ అయ్యుండొచ్చు.. బ్యాంకు స్టేట్‌మెంట్ అయినా సరే... అన్నీ ఎక్కువ శాతం 'పీడీఎఫ్' ఫార్మాట్‌లోనే ఉంటాయి. చూడగానే.. ఆత్రంగా ఎటాచ్ చేసిన ఫైల్ ఓపెన్ చేసేస్తాం!! ఇందులో తప్పేముందీ.. అనుకుంటున్నారా? తప్పేం లేదు గానీ.. మీరు ఓపెన్ చేసిన పీడీఎఫ్ ఫైల్‌లోనే మాల్వేర్ ఉండొచ్చు. అది మీకు తెలియకుండా సిస్టమ్, ఫోన్, ల్యాపీల్లో సైలెంట్‌గా సెటిల్ అయిపోతుంది. అందుకే పీడీఎఫ్‌తో కాస్త జాగ్రత్త అని హెచ్చరిస్తున్నారు సైబర్ నిపుణులు. ముఖ్యంగా కార్పొరేట్ కంపెనీల్లో పని చేసేవాళ్లు. బీ అలర్ట్!! మీ ఇన్‌బాక్స్‌కి చేరే వాటిలో మోసపూరితమైన పీడీఎఫ్‌లు కూడా ఉండొచ్చు!!!

నెటిజన్ల మీద జరుగుతున్న సైబర్ దాడుల్లో '82 శాతం పీడీఎఫ్ ఫైల్స్ అస్త్రంగా చేస్తున్నవే' అని ఇటీవల ఓ సంస్థ నిర్వహించిన అధ్యయనంలో తేలింది. వీటిలో 66 శాతం ఇ-మెయిల్స్ రూపంలో వచ్చి సమాచారం కొల్లగొట్టాయట! ఈ ఫైల్స్‌లో ఉన్న మాలిషియస్ కోడ్ నెటిజన్ల డేటాను అమాంతం లాగేస్తున్నదట. వినియోగదారుల నిర్లిప్తతను ఆసరాగా చేసుకొని తెగబడుతున్నారు సైబర్ మాయగాళ్లు. అర్థం కాని లింకులు, రెగ్యులర్‌గా ఫోన్స్ చేస్తే.. అప్రమత్తం అవుతారనే పీడీఎఫ్ ఫైల్స్‌ను ఎంచుకుంటున్నారు. ఈ ఫైల్స్‌లో మాలిషియస్ కోడ్‌ను నిక్షిప్తం చేస్తున్నారు. రిసీవర్ ఆ అటాచ్‌మెంట్ ఫైల్‌ని ఓపెన్ చేసినా, అందులోని లింక్‌లను క్లిక్ చేసినా మాలిషియస్ కోడ్ యాక్టివేట్ అవుతుంది. సదరు లింకులు ఫిషింగ్ సైట్స్‌కి దారితీయొచ్చు. కొన్నిసార్లు మీ డేటాను దొంగిలించే సాఫ్ట్‌వేర్‌ని మీ డివైజ్‌లో డౌన్‌లోడ్ చేయొచ్చు. కొన్ని పీడీఎఫ్ చిత్రాలు, టెక్ట్స్‌లో ఈ కోడ్ దాగి ఉంటుంది. ఫైల్ ఓపెన్ చేసిన వెంటనే దాడి మొదలవుతుంది. ఫోన్‌బిల్, బ్యాంక్ స్టేట్‌మెంట్, ఎమర్జెన్సీ డాక్యుమెంట్ పేరుతో మెయిల్స్ వస్తాయి. వాటిని ఓపెన్ చేస్తే.. కేటుగాళ్ల ట్రాప్‌లో పడిపోయినట్టే!

ఎవరిని టార్గెట్ చేస్తున్నారు?

సైబర్ నేరగాళ్లు ఎక్కువగా ప్రభుత్వ సంస్థలు, టెక్ కంపెనీలు, డెవలపర్లను టార్గెట్ చేస్తుంటారు. ఎందుకంటే.. ఎక్కువ సంఖ్యలో ఉద్యోగులు ఉండి.. అన్ని రకాల వ్యవహారాలకు పీడీఎఫ్ ఫైల్స్‌ని వాడుతుంటారు. మరోవైపు 'ఏఐ' వాడకం పెరిగిపోవడంతో పీడీఎఫ్‌ను ఆయుధంగా ఎంచుకుంటున్నారు. ఒక సర్వే ప్రకారం.. 2023లో యూజర్లు 40 బిలియన్ పీడీఎఫ్ ఫైల్స్ ఓపెన్ చేశారట. అందులో 16 బిలియన్ ఫైల్స్ ఆర్గనైజేషన్స్‌లో వాడినవి. ఇలా మెయిల్స్ రూపంలో పంపినవాటిలో 87% ఫైల్స్ అడోబ్ ఆక్రోబాట్‌లో ఓపెన్ చేస్తున్నారట. అందుకే ఈ ఫైల్స్‌ని సైబర్ మోసగాళ్లు దాడులకు ఉపయోగిస్తున్నారని నిపుణులు చెబుతున్నారు. ఏదైనా టెక్ కంపెనీలో చేసే ఉద్యోగులకు 'ప్రాజెక్ట్ డాక్యుమెంట్' అని పీడీఎఫ్ ఫైల్ రాగానే చాలామంది వెంటనే దాన్ని ఓపెన్ చేస్తున్నారట. వీటిలో ఒక్క మాలిషియస్ కోడ్ లింక్ ఉన్నా.. దాన్ని క్లిక్ చేసినా కంపెనీ డేటా హుష్ కాకే! అందుకే పీడీఎఫ్ దాడులను ఆపడానికి టెక్ కంపెనీలు రకరకాల రక్షణ వ్యవస్థలను సిద్ధం చేసుకుంటున్నాయి. ఆర్టిఫిషియల్ ఇంటెలిజెన్స్‌తో వాటిని అడ్డుకునే ప్రయత్నం చేస్తున్నాయి.

ఎలా రక్షించుకోవాలి?

- ఫైల్ ఏదైనా సరే ముందు మెయిల్ పంపిన వ్యక్తిని చెక్ చేయండి. తెలియని వాళ్ల నుంచి వచ్చిన PDFలను ఓపెన్ చేయొద్దు.
- పేరుపొందిన కంపెనీలతో ఎలాంటి మెయిల్స్ వచ్చినా కాస్త ఆలోచించండి. 'జాబ్ ఆఫర్స్, క్యాష్ ప్రైజ్‌లు..' అంటూ ఊరించే ప్రయత్నం చేస్తే కచ్చితంగా అది హ్యాకర్ల పనే. అలాంటి యూఆర్ఎల్స్ లేదా పీడీఎఫ్‌లను అస్సలు ఓపెన్ చేయొద్దు.
- సోషల్ మీడియా ప్లాట్‌ఫామ్స్‌లో కనిపించే లింక్‌లను ఓపెన్ చేసి వాటి ద్వారా యాప్స్‌ని ఇన్‌స్టాల్ చేయొద్దు.
- అర్థం లేని అక్షరాలతో కొన్ని 'షార్ట్' యూఆర్ఎల్ లింక్‌లు కనిపిస్తే అనుమానించాల్సిందే! అవి ప్రమాదకరమైన సైట్స్‌లోకి రీడైరెక్ట్ అయ్యే ప్రమాదం ఉంది.
- ఫైల్‌లో లింక్, క్యూఆర్ కోడ్ ఉంటే క్లిక్ చేయొద్దు. సురక్షితమైన PDF వ్యూయర్ వాడండి.
- JavaScript ఆప్షన్‌ని డిసేబుల్ చేయండి. ఇది మాలిషియస్ కోడ్‌ని నిలువరిస్తుంది.
- యాంటీవైరస్ సాఫ్ట్‌వేర్‌ని ఎప్పటికప్పుడు అప్‌డేట్ చేయడం చాలా అవసరం.

వాటితోనే వల పన్నుతారు!

సైబర్ దొంగలు రెండు రకాల కోడ్లను వాడతారు. ఒకటి URL దాడులు. PDFలో ఒక లింక్ ఉంటుంది. క్లిక్ చేస్తే అది ఫిషింగ్ సైట్‌కి వెళ్లిపోతుంది. అక్కడ లాగిన్ డీటెయిల్స్, మీ డేటా దొంగిలిస్తారు. ఇక రెండోది QR కోడ్ దాడులు. PDFలో QR కోడ్ ఉంటుంది. దాన్ని స్కాన్ చేస్తే అది హానికరమైన సైట్‌కు దారితీస్తుంది. ఇలాంటి దాడులు ఎక్కువగా Google, LinkedIn, Microsoft లాంటి ప్రముఖ సంస్థల పేర్లతో వస్తాయి. 'మీ ఖాతా అప్‌డేట్ చేయండి' అని మెయిల్ వస్తుంది. నమ్మి క్లిక్ చేస్తే.. సమస్యల్లో చిక్కుకున్నట్టే! ఈ తరహా దాడుల్లో సాధారణ వ్యక్తుల కంటే కంపెనీలకే రిస్క్ ఎక్కువ. అందుకే ఫ్రాడ్‌స్టర్లు సోషల్ ఇంజనీరింగ్ ద్వారా ఉద్యోగులను టార్గెట్ చేస్తున్నారు. కాబట్టి, పీడీఎఫ్ కంటపడగానే ఏదో పడిపోయినట్టు మరుక్షణంలో క్లిక్ చేయొద్దు. మెయిల్ ఎవరు పంపారు, ఎక్కడినుంచి వచ్చింది తెలుసుకున్న తర్వాతే ఓపెన్ చేయడం శ్రేయస్కరం.

అనిల్ రాచమల్ల
వ్యవస్థాపకులు
ఎండ్‌నౌ ఫౌండేషన్