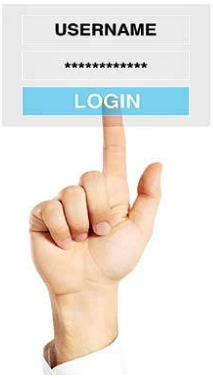
తాళాలు లాగేస్తున్నారు

ఈ-అతిథి



నెట్టింట్లో సంచరిస్తున్నారంటే..

కచ్చితంగా సెక్యూరిటీ చిట్కాల్ని పాటించాల్సిందే.

లేకుంటే తిప్పలు తప్పవని పలు సెక్యూరిటీ సంస్థలు హెచ్చరిస్తున్నాయి. ఎందుకంటే.. గత ఏడాదితో పోలిస్తే లాగిన్ తాళాల్ని దొంగిలించే స్పైవేర్ దాడులు ఈ ఏడాదిలో 60 శాతం పెరిగాయట. గత ఏడాది మొదటి ఆరు నెలల్లో 6,00,000 దాడులు జరిగితే.. ఈ ఏడాది 9,40,000 సైబర్ దాడులు చోటు చేసుకున్నాయి. ఆన్‌లైన్ ప్రైవసీని కోల్పోవడంలో రష్యా తర్వాత మనదే (భారత్) రెండో స్థానం. ఈ నేపథ్యంలో వ్యక్తిగత డేటాపై స్పైవేర్‌లు ఎలా దాడులకు దిగుతున్నాయ్? వాటికి చిక్కకుండా ఎలాంటి రక్షణ చర్యలు తీసుకోవాలి? అనేవి తెలుసుకోవడం అత్యవసరం.

బ్రౌజరే కీలకం..

వినియోగదారుల పాస్‌వర్డ్‌లను దొంగిలించేందుకు సైబర్ నేరగాళ్లు 'పాస్‌వర్డ్ స్టీలింగ్‌వేర్' (పీఎస్‌డబ్ల్యు) టూల్‌కిట్‌లను ఎక్కువగా వాడుతున్నారు. ఈ మాలిషియస్ ప్రోగ్రామ్‌లు పలు మార్గాల ద్వారా యూజర్ల వెబ్ బ్రౌజర్లలోకి చొరబడి మాటేస్తాయి. వీటన్నింటి ఫోకస్ ఒక్కటే యూజర్ వ్యక్తిగత సమాచారాన్ని సేకరించడం. ఈ-మెయిల్స్, ఆర్థిక వ్యవహారాలకు సంబంధించిన ఎకౌంట్‌ల లాగిన్ వివరాలకు గాలం వేసి పట్టేస్తాయి. యూజర్లు చేసే పొరబాట్లే అందుకు ఆసరా. బ్రౌజర్‌లో ముందే పాస్‌వర్డ్‌లు సేవ్ చేయడం.. లేదంటే 'ఆటోఫిల్'తో టైపింగ్ శ్రమని తగ్గించుకోవడం.. ఇవే యూజర్లు చేస్తున్న ప్రధానమైన తప్పులు. అంతేకాకుండా.. కొందరు కార్డు వివరాల్ని పదే పదే టైప్ చేయకుండా ఆయా వెబ్ సర్వీసుల్లో సేవ్ చేస్తుంటారు. దీంతో స్పైవేర్‌లు తమ పని సులభంగా పూర్తి చేసి హ్యాకర్లకు మొత్తం సమాచారాన్ని చేరవేస్తున్నాయి. మరో రకం స్పైవేర్‌లు ఏం చేస్తాయంటే.. బ్రౌజర్ కుకీస్, యూజర్ ఫైల్స్ నుంచి సమాచారాన్ని సేకరిస్తాయి. అంతేకాదు.. పలు అప్లికేషన్స్ ద్వారా షేర్ చేస్తున్న ఫైల్స్ నుంచి కూడా వ్యక్తిగత డేటాని జల్లెడ పట్టేస్తుంటాయి.

ఆసియాలోనే ఎక్కువ..

గత ఆరు నెలల్లో జరిగిన సైబర్ దాడుల్ని గమనిస్తే యూరప్ తర్వాత ఆసియా దేశాల్లోనే ఎక్కువగా చోటు చేసుకుంటున్నాయి. పలు సెక్యూరిటీ సంస్థలు కూడా తమ సర్వేల్లో ఇదే విషయాన్ని వెల్లడి చేస్తున్నాయి. ఎక్కువ శాతం మాల్వేర్ ఎటాక్‌లు రష్యా తర్వాత భారత్, బ్రెజిల్, జర్మనీ, అమెరికా దేశాల్లో జరుగుతున్నాయట. డిజిటల్ ఇండియా వైపు అడుగులు వేస్తున్న క్రమంలో నెటిజన్‌గా మారుతున్న ప్రతీ ఆధునిక సిటిజన్లు ఆన్‌లైన్‌లో చురుకైన పాత్ర పోషిస్తున్నారు. రోజువారీ పనుల్ని ఎక్కువగా నెట్టింట్లోనే చక్కదిద్దుకుంటూ వర్చువల్ లైఫ్‌లోనే ఎక్కువగా గడుపుతున్నారు. దీంతో పుట్టిన తేదీ, జెండర్, అడ్రస్, ఫోన్ నెంబర్లు.. లాంటి మరిన్ని వ్యక్తిగత వివరాలతో డిజిటల్ ప్రొఫైల్‌ని పూర్తి స్థాయిలో మేనేజ్

చేస్తున్నారు. దీంతో ఇంటర్నెట్ ప్రపంచంలో వినియోగదారుడే ఓ హాట్‌కేక్‌లా సైబర్ నేరగాళ్లకు లక్ష్యంగా మారాడు. కట్టుదిట్టమైన రక్షణ వ్యవస్థ లేకుండా లాగిన్ తాళాలు, కార్డు వివరాలు, ఇతర ముఖ్యమైన సమాచారాన్ని బ్రౌజర్లతో భద్రం చేయడం ఎంత మాత్రం సురక్షితం కాదు. సెక్యూరిటీ పరమైన చర్యలు తీసుకునే వెబ్ విహారం చేస్తే మంచిది.

ఇవి గుర్తుంచుకోండి

* నెట్‌కి అనుసంధానమైన ఎలాంటి సర్వీసు నుంచి లాగిన్ వివరాల్ని ఇతరులకు షేర్ చేయొద్దు.

* నకిలీ సైట్‌లతో జాగ్రత్త. యూఆర్ఎల్ లింక్‌లో 'హెచ్‌టీటీపీఎస్' ఉంటేనే లాగిన్ అవ్వండి. 'ఎస్' అంటే సెక్యూర్డ్ అని అర్థం.

* టొరెంటింగ్ సైట్‌లకు దూరంగా ఉండాలి. వీటి ద్వారా మాల్వేర్‌లను పంపడం చాలా సులభం. ఫైల్ షేరింగ్ సర్వీసు ఏదైనా ప్రమాదకరమే. డౌన్‌లోడ్ చేసే ఫైల్‌తో పాటే మాల్వేర్ సిస్టంలోకి ప్రవేశించి కంప్యూటర్ మొత్తాన్ని తన కంట్రోల్‌లోకి తీసుకుంటుంది.

* పబ్లిక్ వై-ఫైలను వాడొద్దు. ఒకవేళ వాడాల్సివస్తే వర్చువల్ ప్రైవేటు నెట్‌వర్క్ (వీపీఎన్) క్రియేట్ చేసుకునే వాడండి. దీంతో మీ 'ఐపీ అడ్రస్' ఎవరి కంటా పడదు. ఉచితంగా అందుబాటులో ఉన్న వీపీఎన్ సర్వీసుల్ని వాడకపోవడం మంచిది. ఎందుకంటే... మీ నుంచి సేకరించిన డేటాతో వాళ్లు సొమ్ము చేసుకోవచ్చు.

* కుకీస్‌ని ఎప్పటికప్పుడు తొలగించాలి. ఎందుకంటే.. పాకెట్స్ రూపంలో సమాచారం కుకీస్‌లో నిక్షిప్తం అవుతుంది. ఉదాహరణకు ఏదైనా ఆన్‌లైన్‌లో ఆర్డర్ చేస్తే షాపింగ్ కార్ట్‌కి సంబంధించిన సమాచారం ఓ పాకెట్‌లో ఉండొచ్చు. ఇలా మీకు సంబంధించిన సమాచారం ఏదైనా స్టోర్ అవ్వొచ్చు.

* లేటెస్ట్ మాల్వేర్‌లు, ఇతర సైబర్ దాడుల్ని ఎదుర్కొనేలా వాడుతున్న యాంటీవైరస్ ఎప్పటికప్పుడు అప్‌డేట్ చేస్తుండాలి.

* ఓఎస్‌ని అప్‌డేట్ చేయడంలో అశ్రద్ధ వద్దు. ఎందుకంటే.. వాడుతున్న కంప్యూటర్ ఏదైనా ఆపరేటింగ్ సిస్టం అప్‌టూడేట్‌గా ఉంటేనే సైబర్ దాడుల్ని అడ్డుకుంటుంది.

* పాస్‌వర్డ్‌లు, ఇతర వ్యక్తిగత సమాచారాన్ని భద్రం చేసుకునేందుకు అధికారిక సెక్యూరిటీ వేదికల్ని మాత్రమే వాడాలి. ఉచితంగా అందిస్తున్నారనే ఆశతో థర్డ్‌పార్టీ సర్వీసుల్లో లాగిన్ వివరాల్ని భద్రం చేయడం ప్రమాదమే.

* వెబ్ ఎంత సెక్యూర్డ్ అయినప్పటికీ మీ పని పూర్తయ్యాక కచ్చింగా లాగ్ అవుట్ చేయాలి. అప్పుడే మీకు సంబంధించిన మూలాల్ని బ్రౌజర్ నుంచి లాగ్‌అవుట్ చేసినట్టు అవుతుంది.

* ఎకౌంట్‌లో ఏవైనా మార్పుల్ని గమనిస్తే వెంటనే పాస్‌వర్డ్‌ని మార్చేయండి. పాస్‌వర్డ్ క్లిష్టంగా ఉండేలా చూసుకోవాలి. ఒకవేళ గుర్తుంచుకోవడం కష్టం అనుకుంటే నమ్మకమైన పాస్‌వర్డ్ మేనేజర్ టూల్స్‌ని వాడొచ్చు.

* వాడుతున్న బ్రౌజర్ ఏదైనా సెట్టింగ్స్‌లోకి వెళ్లి ప్రైవసీని గుట్టుగా మేనేజ్ చేసుకునేందుకు తగిన మార్పులు చేసుకోవాలి. 'ప్రైవసీ అండ్ సెక్యూరిటీ' సెట్టింగ్స్ అందుకు ప్రత్యేకం.

* యాంటీవైరస్, యాంటీ స్పైవేర్‌లతో పాటు సిస్టం ఫైర్‌వాల్స్‌ని కట్టుదిట్టంగా సెట్ చేసుకోవాలి.

కోటిరెడ్డి సరిపల్లి, ఐటీ నిపుణుడు