షార్ట్‌లింక్స్ షాకివ్వొద్దంటే..

స్మార్ట్‌ఫోన్‌లో మెసేజ్.. చూస్తే, ఆకర్షణీయమైన ఆఫర్. జాక్‌పాట్ కొట్టాలంటే కింద ఉన్న లింక్ క్లిక్ చేయమని మెసేజ్ సారాంశం. దాన్ని నొక్కిన వాళ్లెవరూ.. ఆ తర్వాత సుఖంగా నిద్రపోయిన దాఖలాలు లేవు! ఇంతకీ దాన్ని క్లిక్ చేస్తే ఏమవుతుంది?!

శ్రీకాంత్ ఇంజినీరింగ్ చేశాడు. ఉద్యోగం కోసం ఎదురుచూస్తున్నాడు. ఒకరోజు అతనికి ఇ-మెయిల్‌లో ఓ లింక్ వచ్చింది. అందులో 'ప్రముఖ కంపెనీలో ఉద్యోగం' అంటూ ఆఫర్ ఉంది. క్లిక్ చేయగానే, రిజిస్ట్రేషన్ ఫీజు కట్టాలని అడిగారు. శ్రీకాంత్ డబ్బులు కట్టాడు. ఆ తర్వాత కంపెనీ నుంచి ఎలాంటి సమాచారం లేదు. అప్పటికి గానీ తను మోసపోయానని అతనికి అర్థం కాలేదు!!

సుమతికి ఆన్‌లైన్ షాపింగ్ అంటే చాలా ఇష్టం. ఓ రోజు ఎఫ్‌బీలో 'తక్కువ ధరకే చీరలు' అని ఊరించే ఆఫర్ కనిపించింది. లింక్ క్లిక్ చేయగానే, వెబ్‌సైట్ ఓపెన్ అయింది. నచ్చిన చీర ఆర్డర్ చేసింది. డబ్బులు చెల్లించింది. కొన్ని రోజుల తర్వాత, పార్సిల్ వచ్చింది. తెరిచి చూస్తే, అందులో నాసిరకం చీర ఉంది!!

ఇంతకీ ఈ మోసాలకి కారణం? ఓ చిన్న షార్ట్‌లింక్. మెసేజ్, ఇ-మెయిల్, వాట్సాప్, ఫేస్‌బుక్.. దేంట్లోనైనా, తక్కువ అక్షరాలతో కనిపించే షార్ట్‌లింక్‌లే ఈ మోసాలకు కారణం. వెబ్‌లింకే కదా.. క్లిక్ చేస్తే ఏమవుతుంది అనుకోవద్దు. ఈ షార్ట్‌లింక్‌లు చాలా ప్రమాదకరమైనవి. సైబర్ మోసాలకు పాల్పడే ఫ్రాడ్‌స్టర్లకు ఇది షార్ట్‌కట్. డిజిటల్ అక్షరాస్యత లేనివాళ్లను టార్గెట్ చేసి నిండా ముంచుతున్నారు. ఫిషింగ్ దాడులకూ ఇదే ప్రధాన మార్గం.

షార్ట్‌లింక్ అంటే ఏమిటి?

సాధారణంగా వెబ్‌లింక్‌లు పెద్దగా ఉంటాయి. ఉదాహరణకు ఆన్‌లైన్ షాపింగ్ చేసే అమెజాన్‌నే తీసుకోండి. దీంట్లోకి వెళ్లాలంటే https://amazon.in/ అని టైప్ చేస్తే సరిపోతుంది. అదే అమెజాన్‌లో ఏదైనా ఉత్పత్తికి సంబంధించిన వెబ్‌లింక్‌ను చూస్తే.. గజిబిజి అక్షరాలతో చాలా పెద్దగా ఉంటుంది. వాటిని చిన్నవిగానూ చేయొచ్చు. అవే షార్ట్‌లింక్‌లుగా ప్రాచుర్యంలోకి వచ్చాయి. tiny url, bitly, గతంలో గూగుల్ shortener కూడా ఈ షార్ట్‌లింక్ సర్వీసుల్ని అందించాయి. వీటిలో రిజిస్టర్ అయ్యి పొడవైన యూఆర్ఎల్స్‌ని చిన్నవిగా చేసి ఎవరికైనా పంపొచ్చు. ఇలా చేయడం వల్ల ప్రయోజనం ఏంటి? అంటారా! వీటి ద్వారా మనం పంపిన లింక్‌లను ఎంతమంది చూశారు? ఎన్ని క్లిక్‌లు వచ్చాయో ట్రాక్ చేయొచ్చు. ఇంకా చెప్పాలంటే.. ఏదైనా సోషల్ మీడియాలో పొడుగ్గా ఉన్న లింక్‌లను షేర్ చేస్తే అంత ఆకట్టుకునేలా ఉండదు. ఇప్పుడు 'ఎక్స్'గా పిలుచుకుంటున్న ట్విట్టర్‌లో ఒకప్పుడు ఎక్కువ అక్షరాలతో ట్వీట్ చేయడం సాధ్యం అయ్యేది కాదు. అలాంటి సందర్భాల్లో తక్కువ అక్షరాలతో లింక్ షేర్ చేయడానికి ఈ షార్ట్‌లింక్స్‌ని వాడుకునే వాళ్లు. వీటిని బ్రాండింగ్ కోసం ఉపయోగించుకునేవాళ్లు.

చీకటి కోణం

ప్రయోజనాలతో పాటు ఈ షార్ట్‌కట్స్ వెనుక సైబర్ నేరగాళ్ల చీకటి కోణాలు చాలానే ఉన్నాయి. వాటితో నెటిజన్లను ఏమార్చుతూ మోసం చేస్తున్నారు. వ్యక్తిగత సమాచారాన్ని దొంగిలించి ఆర్థిక మోసాలకు పాల్పడుతున్నారు. ఈ షార్ట్‌లింక్స్‌లో హానికరమైన వెబ్‌సైట్లను దాస్తున్నారు. అంతేకాదు.. షార్ట్‌లింక్స్‌లో మాల్వేర్‌లను నిక్షిప్తం చేసి వైరస్‌లను వ్యాప్తి చేస్తున్నారు. వీటిని క్లిక్ చేస్తే.. ఫోన్, ల్యాపీ, డెస్క్‌టాప్‌ల్లో మాల్వేర్‌లు మాటేసుకుని కూర్చుని పర్సనల్ డేటాని హ్యాకర్లకు చేరవేస్తాయి. ఇంకా ఇ-మెయిల్స్ ద్వారా ఫిషింగ్ దాడులు చేస్తారు! మెయిల్‌లో వచ్చిన లింక్‌ని క్లిక్ చేస్తే చాలు.. అది నకిలీ వెబ్‌సైట్‌కి డైవర్ట్ అవుతుంది. తెలియక వివరాల్ని ఎంటర్ చేస్తే.. సైబర్ మోసగాళ్లకు చిక్కినట్టే! ఈ షార్ట్‌లింక్స్‌తో డివైస్‌ని కంట్రోల్‌లోకి తీసుకుని హ్యాకర్లు క్రిప్టో మైనింగ్ ద్వారా డబ్బు దొంగిలిస్తున్నారు కూడా! ■

అనిల్ రాచమల్ల
వ్యవస్థాపకులు
ఎండ్‌నౌ ఫౌండేషన్

ఎలా గుర్తించాలి?

ఎప్పటికప్పుడు అప్రమత్తంగా ఉంటూ.. మీ మెసేజ్ ఇన్‌బాక్స్, వాట్సాప్, ఈమెయిల్‌కి వచ్చిన లింక్‌లను కచ్చితంగా చెక్ చేయాలి. ఈ పాట్టి లింక్స్‌లో దాగున్న డేంజర్స్‌ని పసిగట్టాలి. అందుకు ఆన్‌లైన్‌లో చాలానే సర్వీసులు ఉన్నాయి..

- SMS హెడర్ల తనిఖీ కోసం..
  https://smsheader.trai.gov.in/
- యూఆర్ఎల్స్ గుట్టు విప్పేందుకు..
  www.unshorten.it
  www.checkshorturl.com
  https://www.expandurl.net
- వెబ్‌సైట్ల నిగ్గు తేల్చేందుకు..
  https://isitphishing.org/
  https://www.urlvoid.com/
  https://www.site24x7.com/link-checker.html
  https://transparencyreport.google.com/safe-browsing/search
- ఇమెయిల్ హెడర్ల చెకింగ్..
  https://mxtoolbox.com/EmailHeaders.aspx
  https://dnschecker.org/email-header-analyzer.php
  https://mailheader.org/
  https://www.dmarcanalyzer.com/spf/checker/
- ఫైల్‌వే లేదా యూఆర్ఎల్‌లో ఉన్న వైరస్‌లను వెతికేందుకు..
  https://www.virustotal.com/gui/

- ఇ-మెయిల్స్, SMSలను జాగ్రత్తగా తనిఖీ చేయండి.
- తెలియని లింక్‌లను క్లిక్ చేయొద్దు. సందేహం అనిపిస్తే అధికారిక కస్టమర్ కేర్ సపోర్ట్ తీసుకోవాలి.
- OTP, నెట్ బ్యాంకింగ్ వివరాలు, UPI పిన్‌లను ఎవరితోనూ పంచుకోవద్దు.
- గుర్తు తెలియని లింక్‌లను క్లిక్ చేసి ముందుగానే డబ్బులు చెల్లించవద్దు.
- విక్రేతలు, కొనుగోలుదారుల వివరాలను సరిచూసుకోవాలి. వెబ్‌సైట్, ఆఫీస్ అడ్రస్, ఫోన్ నంబర్లను చెక్ చేయాలి.
- నమ్మకమైన ప్లాట్‌ఫామ్‌ల ద్వారానే చెల్లింపులు చేయాలి.
- తెలియని QR కోడ్‌లు స్కాన్ చేయొద్దు, OTPలు షేర్ చేయొద్దు.
- సైబర్ క్రైమ్ బాధితులైతే https://www.cybercrime.gov.inలో ఫిర్యాదు చేయండి.
- ఆన్‌లైన్‌లో డబ్బులు పోగొట్టుకుంటే 1930 టోల్ ఫ్రీ నెంబర్‌కి కాల్ చేయండి.