విషింగ్... స్మిషింగ్.. ఫిషింగ్.. తస్మాత్ జాగ్రత్త!!

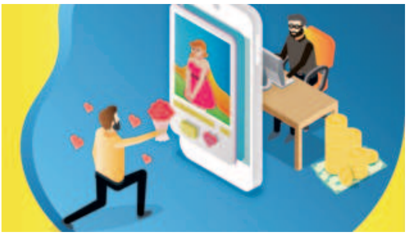
టెక్ టాక్

అరచేతిలోకి స్మార్ట్ ఫోన్ రావడంతోనే మన చుట్టూ ఉన్న ప్రపంచం అంతా డిజిటల్ రూపాన్ని సంతరించుకుంది. అందరాని అద్భుతాలెన్నో అందుబాటులోకి తెచ్చిన సాంకేతికత.. సమస్యలను సృష్టించడంలోనూ ముందుంటున్నది. ఆన్‌లైన్ ప్రపంచంలో అడుగడుగునా పొంచి ఉన్న ముప్పులను పసిగట్టకపోతే తిప్పలు తప్పవు. పేమెంట్ గేట్ వేలోకి కులాసాగా వెళ్లిన వారంతా అంతే దిలాసాగా బయటికి రాలేకపోతున్నారంటే.. ఆన్‌లైన్ ఎంత ప్రమాదకరంగా పరిణమించిందో అర్థం చేసుకోవచ్చు.

మెసేజ్‌లతో మాయ చేస్తారు. కాల్‌తో కొంప ముంచుతారు. ఇ-మెయిల్‌తో ఇల్లు గుల్ల చేస్తారు. సైబర్ నేరగాళ్లు ఎంచుకున్న ఈ మార్గాలకు రకరకాల పేర్లు కూడా ఉన్నాయి. ఫోన్‌కాల్స్‌తో కాటేస్తే విషింగ్ అని, ఎస్సెమ్మెస్‌లతో బోల్తా కొట్టించడాన్ని స్మిషింగ్ అని, ఇ-మెయిల్‌తో బురిడీ కొట్టిస్తే.. ఫిషింగ్ అని పిలుస్తున్నారు. ఏ పేరుతో పిలిస్తేనేం.. సైబర్ మాయగాళ్ల టార్గెట్ అమాయకులే. వాళ్లు చేసే కాల్స్, పంపే సందేశాల బుట్టలో పడ్డామా అంతే సంగతులు! ఊరించే ఆఫర్లతో ఊడిపడే సందేశాన్ని చూసీ చూడగానే సంబురపడిపోయి ఆలోచించకుండా అందులో ఉన్న లింక్‌పై క్లిక్ చేస్తే ప్రమాదమే! ఇలా తలాతోకా లేని నంబర్ల నుంచి వచ్చే మెసేజ్‌లు ఓపెన్ చేసే వారి సంఖ్య 98 శాతం ఉండటం గమనార్హం. వీరిలో పది శాతం మంది అందులో ఉన్న లింక్ ఓపెన్ చేసినా సైబర్ మోసగాళ్ల పంట పండినట్టే!!

బలహీనతే వారి బలం

నమ్మిన చోటే మోసానికి అవకాశం ఉంటుంది. స్కామర్ల సూత్రం కూడా ఇదే! మనుషుల సహజ స్వభావాలే వారి మోసాలకు ఊతమిస్తాయి. గుడ్డిగా నమ్మేవాళ్లనే ముందుగా టార్గెట్ చేస్తారు. భయస్తులు, నిర్లక్ష్యంగా ఉండేవాళ్లు, లోభులు ఇలాంటి వారు దొరికితే ముంచే దాకా వదిలిపెట్టరు. ఫ్రాడ్‌స్టర్లు.. 'మేం మోసం చేయడానికి వచ్చామ'ని చెప్పరు. ప్రొఫెషనల్స్‌గా మాట్లాడతారు. మీ అవసరాన్ని గుర్తించి.. దాన్ని సులభంగా నెరవేరుస్తామని నమ్మబలుకుతారు. అనుమానం రాకుండా మాట తీరుతో గారడి చేస్తారు. బ్యాంకు అధికారులుగానో, కస్టమర్ ఎగ్జిక్యూటివ్‌గానో మాటలు కలిపి ఖాతాలోని సొమ్ముమూటను కాజేస్తారు. ఆఫ్‌లైన్ సందేశాలు, వాట్సాప్ మెసేజ్‌లతో కనికట్టు చేసి నిండా ముంచేస్తారు.



మోసాలు రకరకాలు..

- 'మీ అకౌంట్‌లో రూ.3,00,000 క్రెడిట్ కావడానికి సిద్ధంగా ఉన్నాయి. కింద పేర్కొన్న లింక్ ద్వారా మీ వివరాలు పంపండి' అని సందేశం వస్తుంది. అప్పనంగా మూడు లక్షలు వస్తున్నాయి కదా అని లింక్ ఓపెన్ చేశారో.. మీ ఖాతా ఖాళీ అవుతుంది.
- 'ఫ్లాష్ ఫ్లాష్.. వెంటనే మీ కరెంటు బిల్లు కట్టండి.. గొప్ప రాయితీ పొందండి' అని ఊరించే సందేశం వస్తుంది. ఆఫర్ భలేగా ఉందని తొందరపడి లింక్ మీద వేలు పెట్టారో షాక్ కొట్టడం ఖాయం.
- బ్యాంకు నుంచి వచ్చినట్టుగా కొన్ని ప్రొఫెషనల్ సందేశాలు వస్తుంటాయి. అకౌంట్ వివరాలు సహా జత చేస్తూ.. 'మీ ఖాతాను బ్లాక్ చేస్తున్నాం. ప్లీజ్ అప్‌డేట్ యువర్ పాన్ కార్డ్' అని లింకులు జతచేస్తారు. అకౌంట్ బ్లాక్ అవుతుందేమోనని తొందరపడి లింక్ ఓపెన్ చేసి, ఖాతా వివరాలు ఎంటర్ చేశారా.. అకౌంట్‌లో ఉన్న డబ్బులు కరిగిపోతాయి.
- క్రెడిట్ కార్డు బిల్లు పెండింగ్ అంటూ సందేశాలు వస్తుంటాయి. పెండింగ్ బిల్ ఉంటే అఫీషియల్ యాప్ ద్వారా పే చేయాలి. సందేశాల్లోని లింకుల ద్వారా కడతామంటే.. ఇబ్బందులు పడతారు.
- అన్నిటికన్నా ప్రమాదమైనది రొమాన్స్ స్కామ్. 'ఆర్ యూ ఫీలింగ్ అలోన్.. ఫర్ ఫ్రెండ్‌షిప్, డేటింగ్.. పార్ట్‌నర్ ఈజ్ వెయిటింగ్ ఫర్ యూ.. కాల్' అంటూ మాయ చేస్తారు. ఉచ్చులో చిక్కుకున్నారా.. బ్లాక్‌మెయిల్ చేసి కుచ్చుటోపీ పెడతారు.
- లాటరీ వచ్చిందనీ నమ్మించి ముంచే సందేశాలు కొన్ని.. ఇలా రకరకాలుగా మోసాలకు పాల్పడుతూనే ఉంటారు. ఏ కాస్త ఏమరుపాటుగా ఉన్నా.. నిండా ముంచేస్తారు. ■

ఇలా చెక్ పెట్టండి..

- https://unshorten.it లింక్ ద్వారా మెసేజ్‌లలోని యూఆర్ఎల్ లింక్స్ సోర్స్ తెలుసుకోవచ్చు.
- isitphishing.org, www.urlvoid.com వెబ్‌సైట్‌ల సాయంతో మీకు వచ్చే సందేశంలోని వెబ్ లింక్స్ సరైనవో కాదో తెలుసుకోవచ్చు. ఫిషింగ్ లింక్ అని తేలితే.. మీ వ్యక్తిగత వివరాల విషయంలో గోప్యత పాటించడం అత్యవసరం.
- https://smsheader.trai.gov.in లింక్ ద్వారా ఎస్సెమ్మెస్ యాక్చువల్ సెండర్ వివరాలు తెలుసుకోవచ్చు.
- https://reports.exodus-privacy.eu.org/en లింక్‌ను ఉపయోగిస్తే... మీరు వాడుతున్న యాప్స్ మీ డాటాను ఎలా యాక్సెస్ చేస్తున్నాయో తెలుసుకోవచ్చు. అనుమానాస్పదంగా ఉంటే ఆయా అప్లికేషన్లను వెంటనే అన్ ఇన్‌స్టాల్ చేయడం మంచిది.
- కస్టమర్ కేర్ నంబర్లను సెర్చ్ ఇంజిన్స్‌లో ఎప్పుడూ వెతక్కండి. అఫీషియల్ వెబ్‌సైట్ల ద్వారా నంబర్ తెలుసుకోండి.
- ఓటీపీ, సీవీవీ నంబర్ ఎవరికీ షేర్ చేయకండి.
- ఆన్‌లైన్‌లో ఏదైనా మోసానికి గురైతే వెంటనే స్థానిక పోలీసులకు ఫిర్యాదు చేయండి. https://www.cybercrime.gov.inలో ఫిర్యాదు రిజిస్టర్ చేయండి. 1930 నంబర్‌ను సంప్రదించి కూడా ఫిర్యాదు చేయొచ్చు.

అనిల్ రాచమల్ల
వ్యవస్థాపకులు
ఎండ్‌నౌ ఫౌండేషన్