సైబర్ మోసాలు మరియు నేరాలపై అవగాహన

సైబర్ ప్రపంచం రెండు వైపులా పదునున్న కత్తిలాంటిది. సైబర్ నేరగాళ్లు సైబర్ క్షేత్రాన్ని దుర్వినియోగం చేసి ప్రపంచ భద్రతను ప్రమాదంలోకి నెట్టేస్తున్నారు. ఎక్కడో సుదూర ప్రాంతంలో ఉన్న సైబర్ నేరస్తులు మన నెట్టింట్లో ప్రవేశించి మన బ్యాంకు ఖాతాను ఖాళీ చేసేస్తున్నారు. మన ప్రైవసీని దెబ్బ తీస్తున్నారు.

సైబర్ క్రైమ్ అనేది కంప్యూటర్ ఆధారిత నేరం. కంప్యూటర్, కంప్యూటర్ నెట్‌వర్క్, నెట్‌వర్క్ డివైజ్‌లే లక్ష్యంగా చేసే దాడి లేదా నేరపూరిత చర్యను సైబర్ క్రైమ్ అంటారు. అక్రమంగా డబ్బు సంపాదించాలనుకునే సైబర్ నేరగాళ్లు, హ్యాకర్లు.. ఇలాంటి నేరాలకు పాల్పడతారు. వ్యక్తులు లేదా సంస్థలు ఒక ప్రణాళిక ప్రకారం ఉమ్మడి లక్ష్యం కోసం ఈ రకమైన మోసాలు చేయాలనుకుంటారు. ఒక వ్యక్తి, సంస్థ లేదా దేశ రక్షణకు, ఫైనాన్షియల్ హెల్త్‌కు సైబర్ నేరాలు ఆటకం కలిగిస్తాయి. ఇలాంటి చర్యలు చట్టవ్యతిరేకమైనవి. భారత్‌తో పాటు ప్రపంచ దేశాలు సైబర్ నేరాలకు కఠినమైన శిక్షలు విధిస్తున్నాయి

సైబర్ నేరం అంటే ఏంటి?

కంప్యూటర్‌ను సాధనంగా లేదా తదుపరి నేరాలకు పాల్పడే మార్గంగా ఉపయోగించే అన్ని రకాల నేరపూరిత చర్యలు సైబర్ నేరాల కిందకు వస్తాయి. కంప్యూటర్ ద్వారా మోసాలకు పాల్పడటం లేదా టెక్నాలజీని ఉపయోగించి కంప్యూటర్లపై దాడి చేయడం.. ఈ రెండూ చట్టవిరుద్ధమైన చర్యలే.

కంప్యూటర్ వనరులను సాధనంగా ఉపయోగించే నేరాలు

సైబర్ క్రైమ్ ప్రధాన లక్ష్యం వ్యక్తి అయినప్పుడు, కంప్యూటర్‌ను లక్ష్యంగా కాకుండా సాధనంగా పరిగణించవచ్చు. ఈ నేరాలు సాధారణంగా తక్కువ సాంకేతిక నైపుణ్యాన్ని కలిగి ఉంటాయి. మానవ బలహీనతలు సాధారణంగా దోపిడీకి గురవుతాయి. వ్యవహరించిన నష్టం చాలావరకు మానసిక, అసంపూర్తిగా ఉంటుంది, ఇది వేరియంట్‌లపై చట్టపరమైన చర్యలను మరింత కష్టతరం చేస్తుంది. ఆఫ్‌లైన్ ప్రపంచంలో శతాబ్దాలుగా ఉన్న నేరాలు ఇవి. హైటెక్ పరికరాల అభివృద్ధికి ముందే మోసాలు, దొంగతనం,

ఇష్టాలు ఉన్నాయి. అదే నేరస్థుడికి కేవలం ఒక సాధనం ఇవ్వబడింది, ఇది వారి బాధితుల సంభావ్య సమూహాన్ని పెంచుతుంది, వారిని గుర్తించడం, పట్టుకోవడం కష్టతరం చేస్తుంది.

- **<u>మోసం, గుర్తింపు దొంగతనం</u>** (ఇది మాల్వేర్, హ్యాకింగ్ లేదా ఫిషింగ్‌ను ఎక్కువగా ఉపయోగిస్తున్నప్పటికీ, ఇది "కంప్యూటర్ లక్ష్యంగా", "కంప్యూటర్ సాధనంగా" నేరం రెండింటికి ఉదాహరణగా మారుతుంది)
- **<u>ఫిషింగ్ మోసాలు</u> :** సైబర్ మోసం: ఉదాహరణకు, డబ్బు వినియోగదారులను మోసం చేయడానికి తప్పుడు వెబ్‌సైట్‌లను ఏర్పాటు చేయడం లేదా వినియోగదారుల క్రెడిట్ కార్డ్ సమాచారాన్ని మోసం చేయడానికి 'ఫిషింగ్' ఉపయోగించడం
- వేధింపులు, బెదిరింపులతో సహా అక్రమ అశ్లీల లేదా అప్రియమైన కంటెంట్ యొక్క ప్రచారం
- **వైరస్ వ్యాప్తి** - సైబర్ నేరస్థులు వైరస్లు, పురుగులు, ట్రోజన్ గుర్రాలు, లాజిక్ హార్స్ వంటి వైరస్లను కలిగి ఉన్న కొన్ని సాఫ్ట్‌వేర్‌లను మీ కంప్యూటర్‌కు పంపుతారు.
- **సాఫ్ట్‌వేర్ పైరసీ** - సాఫ్ట్‌వేర్‌ను కాపీ చేసి తక్కువ ధరకు అమ్మడం కూడా సైబర్ క్రైమ్ పరిధిలోకి వస్తుంది, ఇది సాఫ్ట్‌వేర్ కంపెనీలకు భారీ నష్టాన్ని కలిగిస్తుంది, మీ విలువైన పరికరాలు సరిగా పనిచేయవు.
- **నకిలీ బ్యాంక్ కాల్** - మీ బ్యాంక్ లాగా కనిపించే నకిలీ ఇమెయిల్, సందేశం లేదా ఫోన్ కాల్ మీకు అందుతుంది, దీనిలో మీ ఎటిఎం నంబర్, పాస్వర్డ్ అవసరం అని అడిగారు, మీరు ఈ సమాచారాన్ని అందించకపోతే, మీరు ఖాతా మూసివేయబడతారు లేదా ఇది దయచేసి లింక్‌పై సమాచారాన్ని అందించండి. అటువంటి సమాచారం ఏ బ్యాంకు అయినా ఈ విధంగా అడగదని గుర్తుంచుకోండి, ఇంటర్నెట్ లేదా ఫోన్ కాల్ లేదా సందేశం ద్వారా ఈ రకమైన సమాచారాన్ని చెప్పడం మర్చిపోవద్దు.
- **సోషల్ నెట్‌వర్కింగ్ సైట్లలో పుకార్లను వ్యాప్తి చేయడం** - చాలా మంది సోషల్ నెట్‌వర్కింగ్ సైట్లలో సామాజిక, సైద్ధాంతిక, మత, రాజకీయ పుకార్లుగా వ్యవహరిస్తారు, కాని వినియోగదారులు వారి ఉద్దేశాలను అర్థం చేసుకోరు, తెలిసి అలాంటి లింక్‌లను పంచుకుంటారు, కానీ ఇది సైబర్ క్రైమ్, సైబర్-టెర్రరిజం వర్గంలోకి వస్తుంది.
- **సైబర్ బెదిరింపు -** ఫేస్‌బుక్ వంటి సోషల్ నెట్‌వర్కింగ్‌పై అసభ్యకరమైన వ్యాఖ్యలు చేయడం, ఇంటర్నెట్‌లో బెదిరింపులు చేయడం, ఎవరైనా బెదిరింపులకు గురిచేసే స్థాయికి ఎగతాళి చేయడం, ఇంటర్నెట్ ముందు ఇతరులను ఇబ్బంది పెట్టడం, దీనిని సైబర్

బెదిరింపు అంటారు. తరచుగా పిల్లలు దీనికి బలైపోతారు. ఇది వారి ఆరోగ్యాన్ని కూడా ప్రభావితం చేస్తుంది.

మోసగాళ్లు ఎన్ని విధాలుగా సైబర్ నేరాలకు పాల్పడే అవకాశం ఉంది?

కంప్యూటర్ సిస్టమ్స్ లేదా నెట్‌వర్క్‌లను అక్రమంగా, అనధికారంగా యాక్సెస్ చేయడం లేదా హ్యాకింగ్ చేయడం, ఎలక్ట్రానిక్ రూపంలో ఉన్న సమాచారాన్ని దొంగిలించడం, ఈ మెయిల్ బాంబింగ్, సలామి ఎటాక్, సర్వీస్ ఎటాక్‌ను అడ్డుకోవడం, వైరస్ లేదా వార్మ్ దాడులు, లాజిక్ బాంబ్స్, ఇంటర్నెట్ టైమ్ థెఫ్ట్స్... వంటివన్నీ వివిధ రూపాల్లో ఉండే సైబర్ నేరాలు.

వివిధ రకాల సైబర్ నేరాలు ఏవి?

ప్రభుత్వానికి వ్యతిరేకంగా చేసే సైబర్ టెర్రరిజం.. వ్యక్తులను లక్ష్యంగా చేసుకునే సైబర్ పోర్నోగ్రఫీ, సైబర్ స్టాకింగ్, సైబర్ డిఫమేషన్.. ఆస్తులను లక్ష్యంగా చేసుకునే ఆన్‌లైన్ గ్యాంబ్లింగ్, మేధో సంపత్తి హక్కుల ఉల్లంఘన, ఫిషింగ్, క్రెడిట్ కార్డు మోసాలు వంటివి వివిధ రకాల సైబర్ నేరాలు.

IP స్పూఫింగ్ అంటే ఏంటి?

కంప్యూటర్లను అనధికారంగా, మోసపూరితంగా యాక్సెస్ చేసేందుకు ఈ టెక్నాలజీని నేరగాళ్లు ఉపయోగిస్తారు. ఈ పద్ధతిలో చొరబాటుదారులు IP హోస్ట్ ఉన్న కంప్యూటర్‌కు కొన్ని రకాల మెస్సేజ్‌లను పంపుతారు. అది ట్రస్ట్ హోస్ట్ నుంచి వస్తున్నట్లు నమ్మిస్తారు. దీని ద్వారా సిస్టమ్‌ను తమ ఆధ్వర్యంలోకి తీసుకుంటారు.

ఫిషింగ్ అంటే ఏమిటి?

వినియోగదారుని పేరు, పాస్‌వర్డ్, క్రెడిట్ కార్డ్ వివరాలు.. వంటి సున్నితమైన సమాచారాన్ని దొంగిలించడానికి చేసే నేరం, మోసపూరిత చర్యను ఫిషింగ్ అంటారు. విశ్వసనీయ సంస్థగా లేదా ఎలక్ట్రానిక్ కమ్యూనికేషన్‌లోని వ్యక్తిగా మారువేషాల ద్వారా ఈ మోసాలకు పాల్పడతారు.

ఫిషింగ్ / సమాచారవేట

- వినియోగదారుల యొక్క గోప్య సమాచారాన్ని నేరుగా వినియోగదారుల నుంచే రాబట్టే ప్రయత్నాన్ని ఫిషింగ్ లేదా సమాచారవేట అంటారు.
- సాధారణంగా వినియోగదారుని పేరు (యుసర్ నేమ్), సంకేతపదాలు (పాస్వ్వర్డ్), ఋణసౌకర్య పత్రాల సంఖ్యలు (క్రెడిట్ కార్డు నంబర్స్) వంటి గోప్య సమాచారాన్ని తెలుసుకోవడానికి ప్రయత్నిస్తూ ఉంటారు నేరగాళ్ళు. పైన వివరించబడ్డ ఈమెయిల్ స్పూఫింగ్ వంటి పద్ధతులు ఈ సమాచారవేటకి ఉపయోగిస్తారు నేరగాళ్ళు.
- ఉదా :- మీ ప్రియస్నేహితుడి పేరు వాడుకొని వేరొకడు మీ క్రెడిట్ కార్డు / ఋణ సౌకర్య పత్రాల సంఖ్యలు కావాలంటూ మీకు ఈమెయిలు చేయడం, మీరు నిజమో కాదో నిర్ధారించుకోకుండా ఆ ఈమెయిలుకి బదులుగా మీ వివరాలు పంపించడం.

సోషల్ ఇంజనీరింగ్ / సామాజిక నైపుణ్య దాడులు

- సామాజిక నైపుణ్య దాడుల లక్ష్యం వినియోగదారుడి పరిధిలో ఉన్న గోప్య సమాచారాన్ని బయటకు చెప్పే విధముగా ఒప్పించడం. ఇది రకరకాలుగా చేయవచ్చు.
- కొంతమంది సామాజిక మాధ్యమాలలో స్నేహాలు పెంచుకుని, ఉరికే అడుగుతునట్టుగా అడగటము ఒక పద్ధతి. గొంతుమర్చి నీ పైఅధికారిని అంటూ కాల్ చేసి వివరాలు అడగటము మరో పద్ధతి. బ్యాంకు నుంచి కాల్ చేస్తున్నామని, ప్రభుత్వం నుంచి కాల్ చేస్తున్నామని ఇలా రకరకాలుగా ఈ మోసాలు చేస్తుంటారు.
- అతి సాధారణంగా జరిగిన సామజిక నైపుణ్య దాడులలో ఒకటి, నేను మీ ప్రధాన కార్యనిర్వహణాధికారినంటూ ఆర్థిక విభాగానికి ఈమెయిలు చేసి తన ఎకౌంటుకి డబ్బులు పంపమని ఆదేశించటం.

లాటరీ మెయిల్స్ వల అంటే ఏమిటి?:

దేశంలో ఆన్‌లైన్ లావాదేవీల వ్యాపారమూ శరవేగంగా విస్తరిస్తోంది. అయినా సైబర్ నేరాలపట్ల ప్రజలకు ఉన్న అవగాహన బాగా తక్కువ. అందుకే లాటరీ తగిలిందని తప్పుడు మెయిల్ పంపించి పెద్దయెత్తున డబ్బు కొల్లగొట్టే నైజీరియన్ మోసాల సంఖ్య ఎక్కువవుతోంది. రూ.కోట్ల విలువ చేసే లాటరీ కలిసిందని చెప్పగానే వెనకాముందు ఆలోచించకుండా అడిగినంత డబ్బు మాయగాళ్ల ఖాతాల్లో డిపాజిట్ చేసేవారి సంఖ్యకూ కొదవలేదు.

తీసుకోవాల్సిన జాగ్రత్తలు:

1. **ఆధునిక పంథాలో అకౌంట్ టేకోవర్:** ఇటీవల ఎక్కువగా నమోదయ్యే నేరాలు అకౌంట్ టేకోవర్‌కు సంబంధించినవే. ఈ సైబర్ నేరగాళ్లు వ్యాపార లావాదేవీలు జరిపే వారి ఈ-మెయిల్స్ ను హ్యాక్ చేస్తారు. అన్ సెక్యూర్డ్ ఈ-మెయిల్ ఐడీల లావాదేవీలను కొంతకాలం పరిశీలిస్తారు. అదును చూసుకుని నగదు చెల్లించాల్సిన వ్యక్తికి, నగదు తీసుకునే వ్యక్తిలా మెయిల్ పంపిస్తారు. బ్యాంక్ ఖాతా మారిందంటూ తమ ఖాతాను మెయిల్‌లో పొందుపరుస్తారు. దీంతో చెల్లింపులు సైబర్ నేరగాడి ఖాతాలోకి వస్తాయి. అందుకే ఖాతాలు మారినట్టుగా సమాచారం వస్తే అవతలి వ్యక్తిని నేరుగా సంప్రదించి నిర్ధారించుకున్న తరవాతే డిపాజిట్ చేయడం ఉత్తమం.
2. **దురాశ వద్దు:** సినిమా హాళ్లు, షాపింగ్ మాల్స్ వంటి చోట్ల ఏదో ఒక సర్వే చేస్తున్నామని నమ్మబలుకుతుంటారు. ఈ-మెయిల్ ఐడీ, సెల్‌ఫోన్ నెంబరు రాసి డబ్బాలో వేస్తే డ్రా తీసి బహుమతి ఇస్తామని కూడా ఆశపెడతారు. అలాంటి వారికి వివరాలిస్తే, ఇబ్బందే. వారి దగ్గర నుంచి ఈ వివరాలను సైబర్ నేరగాళ్లు కొనేసి తమ పని కానిస్తుంటారు.
3. **ఒక్క మెయిల్ తో ఖాతా ఖాళీ:** మేం ఫలానా బ్యాంకు నుంచి మెయిల్ చేస్తున్నాం. భద్రతా చర్యల్లో భాగంగా అందరి వివరాలూ తనిఖీ చేస్తున్నాం. మీ అకౌంట్ నెంబర్, పాస్‌వర్డ్ చెప్తే ఎవరూ టాంపర్ చేయకుండా చర్యలు తీసుకుంటాం. అంటూ వచ్చే ఈ-మెయిల్‌కు స్పందిస్తే ఖాతా ఖాళీ అయిపోయినట్లే. ప్రపంచ వ్యాప్తంగా సైబర్ నేరగాళ్లు రోజుకు ఇలా 98 లక్షల ఫిషింగ్ మెయిల్స్ పంపుతున్నట్లు అంచనా. ఇక ఎస్ఎమ్మెస్‌లో ఇలా వచ్చే సందేశాన్ని స్మిషింగ్ (SMiShing) అంటారు.
4. **కీ లాగర్స్**: కంప్యూటర్ ద్వారా జరిపే ప్రతి లావాదేవీని తెలుసుకునేందుకు కీ లాగర్స్ అనే సాఫ్ట్ వేర్ వాడుతున్నారు. కంప్యూటర్‌ను వినియోగించిన వారు ఏ సమాచారం టైప్ చేశారో ఈ సాఫ్ట్ వేర్‌తో తెలుసుకోవచ్చు. నెట్ కేఫ్‌ల్లోని సిస్టమ్స్ లో వీటిని ఏర్పాటు చేస్తున్నారు. దీనితో కంప్యూటర్‌ను వాడుకున్న వారు టైప్ చేసిన సమాచారాన్ని తస్కరించి దుర్వినియోగం చేసే వాళ్లు పెరిగారు.
5. **క్రెడిట్ కార్డుతో జాగ్రత్త:** షాపు లేదా పెట్రోల్ బంక్ కు వెళ్లి, క్రెడిట్ కార్డుతో బిల్లు చెల్లించినపుడు కార్డు చెల్లింపు సమాచారానికి చెందిన ఒక కాపీ వారే ఉంచుకుంటారు. వారి దగ్గర ఉంచుకునే బిల్లు కాపీలో ఉన్న పేరు, కార్డు నెంబరు ఉంటాయి. కార్డు వెనుక ఉన్న సీవీవీ కోడ్‌ను అవతలి వ్యక్తులు నోట్ చేసుకుంటే. నెట్‌లో మీ ఖాతాతో వారు షాపింగ్ చేసుకోవచ్చు. ఒక్కోసారి స్కిమ్మర్లను వినియోగించి కార్డు డేటాను దొంగిలించి, మరో కార్డు తయారు చేసి జల్సా చేస్తున్నారు.

6. **అవగాహనే కీలకం:** ఈ కేసుల్లో నిందితులను పట్టుకోవడం దాదాపు అసాధ్యం కాబట్టి, వీటిపై ప్రభుత్వం ప్రజల్లో అవగాహన కల్పించాలి. కళాశాలలు, కార్యాలయాల్లో విస్తృతంగా ప్రచారం చేయాలి.

సైబర్ నేరాలపై ఎవరికి ఫిర్యాదు చేయాలి?

సైబర్ దాడులకు గురైనవారు సైబర్ క్రైమ్ ఇన్వెస్టిగేషన్ సెల్ సంఖ్య 1930 కు ఫిర్యాదు చేయాల్సి ఉంటుంది. బాధితుల పేరు, మెయిలింగ్ అడ్రస్, ఇతర వివరాలను ఫిర్యాదులో పేర్కోవాలి. నేరం ఎలా జరిగిందనే అంశాన్ని పూర్తిగా నమోదు చేయాలి. అత్యవసరమైతే స్థానిక పోలీస్ స్టేషన్‌ను సంప్రదించవచ్చు.